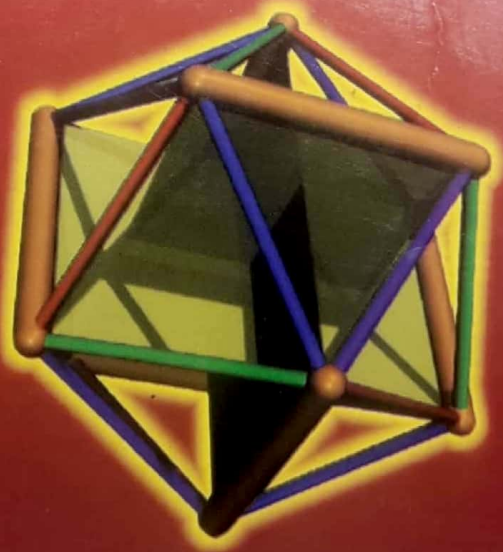
Z.R. Bhatti

Basic

GROUP THEORY

d Edition

For B.A./B.Sc.
BS 4-Years
M.Sc. Mathematics



ILMI KITAB KHANA
Kabir Street, Urdu Bazar, Lahore.

Contents

Chapter

1

SETS, FUNCTIONS AND BINARY OPERATIONS

Set theory has been usefully employed in various branches of natural sciences. It forms a basis of all the fundamental concepts of mathematics specially, topology, real analysis, functional analysis, algebra and group theory. Set theory also plays a key role in solving the problems of applied mathematics, physics, chemistry and many other scientific disciplines. It is obviously impossible to give a complete discussion on various aspects of set theory and its uses in the different scientific disciplines in this elementary book. However, some basic concepts concerning to group theory are presented in this introductory chapter.

1-1 Definitions and Set Operations

1-1.1 Definition: The collection of well defined objects is called a *set*. The well defined objects of this collection are said to be the *elements* or *points* of the set. Sets are denoted by capital letters while their elements are denoted by small letters. If x is an element of the set A, we write $x \in A$ and read 'x belongs to A'. If x is not an element of a set A, we write $x \notin A$ and read 'x does not belong to A'.

If A is a set and P is a statement which applies to some of the elements of A, then the set of elements x of A for which $P(x)$ is true is denoted by $\{x \in A : P(x)\}$.

Thus if N is the set of positive integers, the positive divisors of 16 form the set $\{x \in N : xy = 16, \text{for some } y \in N\}$. In the case of small sets it is easy to describe the set by listing its elements in brackets. Thus the set just given above is the set $\{1,2,4,8,16\}$. The three ways of writing sets are given in the following definitions.

1-1.2 Definition: A set can be expressed by descriptive statement and this way of expressing a set is called the *descriptive method*. For example, first hundred natural numbers, students in the college, the positive integers which are divisible by 2 etc.

1-1.3 Definition: If we list the elements of the set by writing them within braces, then this method of writing a set is said to be the *tabular method*. For example, the set of first ten positive even integers is written as

$$\{2, 4, 6, 8, 10\}$$

1-1.4 Definition: If we describe a set by stating a characteristic property which identifies all the elements of the set then this method is said to be *set builder method*. For example,

$$A = \{x : x \text{ is an integer betw een 10 and 20}\}$$

$$B = \{x : x \text{ is a BS student of GCS during 2014}\}$$

Usually the following symbols are used for sets of numbers:

The set of real numbers	R
The set of complex numbers	C
The set of integers	Z
The set of even integers	E
The set of positive integers (natural numbers)	N
The set of rational numbers	Q

1-1.5 Examples:

1. The set M of students in a class of Mathematics is represented by $M = \{s : s \text{ is a student of a class of mathemtics }\}$
2. The set T of BS students of FCC during 2014 is represented by $T = \{s : s \text{ is a BS student of FCC during 2014}\}$
3. The set C_4 consisting of complex numbers $\pm i, \pm 1$ is represented by $C_4 = \{-i, i, -1, 1\}$
4. The solution set S of cubic equation is represented by $S = \{\alpha \in C : \alpha \text{ is a solution of } a_0x^3 + a_1x^2 + a_2x + a_3 = 0, a_0 \neq 0\}$
5. The set of all points on a circle of radius one and centre zero is written as $P = \{(x, y) : x, y \in R, x^2 + y^2 = 1\}$.
6. The set of all points on a line $y = mx + c$ is written as $L = \{(x, mx + c) : m, c, x \in R \text{ and } m, c \text{ are fixed}\}$

1-1.6 Definition: A set which contains no elements is called an *empty set* or *vacuous set* or *null set*. It is denoted by ϕ.
The symbol ϕ is read as phi.

This definition of empty set seems to contradict the definition of a set but this apparent contradiction disappears when we understand the meanings of well defined objects. By the well defined objects we mean that the objects which can be considered as the members of the set under consideration. For example, a cup is not a well defined object for a sofa set. Similarly, a chair is not a well defined object for a water set. But if we consider the set of necessary things of a house, then both of above mentioned things are well defined objects for such a set.

Thus, if an object does not exist then it is a well defined object for an empty set. For example, odd numbers which are divisible by 2 are well defined objects for an empty set. Similarly, the positive integers which are less than -1 are also well defined objects for an empty set. If Z^+ denotes the set of all positive integers, then the last set may be represented as

$$\phi = \{x : x \in Z^+ \text{ and } x < -1\}$$

1-1.7 Definition: A set A is said to be the *subset* of a set B if every element of A is also an element of B; and we express this fact by writing $A \subset B$. In this case we say that A is contained in B or B contains A. If A is a subset of B and B has at least one element which is not in A, then A is called the *proper subset* of B.

For example, $A = \{2, 4, 6, 8, 10\}$ is a proper subset of $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

If A is a subset of B, then B is called the *superset* of A. The symbol $\subset$ is called the *inclusion symbol*. If A is not a subset of B we write $A \not\subset B$. By the definition of a subset it is clear that the empty set and the set A itself are always subsets of A. These two subsets are called the *improper subsets* of A.

1-1.8 Definition: Two sets A and B are said to be *equal* if $A \subset B$ and $B \subset A$. In this case we write $A = B$. If there is at least one element of B which is not in A, then A is not equal to B and we write $A \neq B$.

1-1.9 Definition: The *difference* $A - B$ of two sets A and B is defined to be set of those elements of A which are not in B. Thus, $A - B = \{x \in A : x \notin B\}$.

For example, if

$$A = \{1, 2, 3, 4, 5, 6, 7, 8\},\ B = \{1, 3, 5, 7, 9\},$$

then

$$A - B = \{1, 2, 3, 4, 5, 6, 7, 8\} - \{1, 3, 5, 7, 9\}$$
$$= \{2, 4, 6, 8\}$$

1-1.10 Definition: If $B \subset A$, then $A - B = \{x \in A : x \notin B\}$ is said to be the *complement* of B in A. This definition shows that the complement of a set A in A is an empty set. The complement of a set A is usually denoted by A^c.

1-1.11 Definition: The *union* of two sets A and B is a set whose elements are elements of A or of B. It is denoted by $A \cup B$. Thus the union of two sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$ It is clear that the union of two sets is always the superset of both sets, i.e.

$$A \subset A \cup B, \quad B \subset A \cup B$$

1-1.12 Definition: The *intersection* of two sets A and B, denoted by $A \cap B$, is a set whose elements are in both A and B. Thus the set of common points of sets A and B is said to be their intersection. It is clear that the intersection of two sets is a subset of both sets, i.e. $A \cap B \subset A, A \cap B \subset B$.

In the set builder form the intersection of two sets is given by $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

1-1.13 Definition: Two sets A and B are said to be *disjoint* if they have no common points, i.e. $A \cap B = \phi$. We express this by saying that A *does not intersect* B. If $A \cap B \neq \phi$, we express this by saying that A *intersects* B.

1-1.14 Definition: Given a set I, if for each $\alpha \in I$, there is a set A_α, then $\{A_\alpha : \alpha \in I\}$ is called an *indexed family of sets* and the set I is called the *indexing set*.

For an indexed family of sets, their union and intersection are given below:

$$\bigcup_{\alpha \in I} A_\alpha = \bigcup \{A_\alpha : \alpha \in I\} = \{x : x \in A_\alpha \text{ for some } \alpha \in I\}$$

$$\bigcap_{\alpha \in I} A_\alpha = \bigcap \{A_\alpha : \alpha \in I\} = \{x : x \in A_\alpha \text{ for all } \alpha \in I\}$$

Similarly, the union and intersection of sets $A_1, A_2, \ldots$ are respectively written as $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.

1-1.15 Definition: If all the under consideration sets are assumed to be the subsets of a single fixed set then this fixed set is said to be the *universal set* and is usually denoted by U. Thus, while taking complements, unions, and intersections it is assumed that there is some universal set with respect to which we perform these operations.

1-1.16 De Morgan Laws: *If A and B are subsets of a universal set U, then* (i) $(A \cup B)^c = A^c \cap B^c$

(ii) $(A \cap B)^c = A^c \cup B^c$.

Proof: (i) Let $x \in (A \cup B)^c$

$\Rightarrow x \notin (A \cup B)$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \in A^c$ and $x \in B^c$

$\Rightarrow x \in A^c \cap B^c$

$\Rightarrow (A \cup B)^c \subseteq A^c \cap B^c$ ...(1)

Conversely, let $x \in A^c \cap B^c$

$\Rightarrow x \in A^c$ and $x \in B^c$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \notin A \cup B$

$\Rightarrow x \in (A \cup B)^c$

$\Rightarrow A^c \cap B^c \subseteq (A \cup B)^c$ ...(2)

Combining (1) and (2), we have

$(A \cup B)^c = A^c \cap B^c$

(ii) Let $x \in (A \cap B)^c$

$\Rightarrow x \notin (A \cap B)$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \in A^c$ or $x \in B^c$

$\Rightarrow x \in A^c \cup B^c$

$\Rightarrow (A \cap B)^c \subseteq A^c \cup B^c$ ...(3)

Conversely, let $x \in A^c \cup B^c$

$\Rightarrow x \in A^c$ or $x \in B^c$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in (A \cap B)^c$

$\Rightarrow A^c \cup B^c \subset (A \cap B)^c$ ...(4)

Combining (3) and (4), we have

$(A \cap B)^c = A^c \cup B^c$

1-2 Relations

If x and y are distinct elements of some set, the two-element sets $\{x, y\}$ and $\{y, x\}$ are the same, because, each of these sets is a subset of the other. It is useful to have a device for reflecting priority as well as membership in this case, and it is provided by the notion of the *ordered pairs* (x, y). By definition ordered pairs (x, y) and (a, b) are equal if and only if $x = a$ and $y = b$. Thus $(x, y) = (a, b) \Leftrightarrow x = a, y = b$.

1-2.1 Definition: Let A and B be two nonempty sets, then the set consisting of all ordered pairs (a, b), where $a \in A$ and $b \in B$, is called the *Cartesian product* of A and B and is denoted by $A \times B$.
Thus, $A \times B = \{(a,b): a \in A, b \in B\}$.

For example, if $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then
$$A \times B = \{(1, a), (2, a), (3, a), (1, a), (2, b), (3, b)\}$$

1-2.2 Definition: A subset R of $A \times B$ is called a *binary relation* or simply a *relation* from A to B. If a pair $(a, b) \in R$, then a is said to be an R-relative of b and is written as $a\ R\ b$. If $(a, b) \notin R$, then we write aRb (read as 'a is not an R-relative of b'). If $B = A$, then we say that R is a relation in A.

1-2.3 Definition: A relation R from A to B is said to be *empty* or *nullary* if $R = \phi$ and *full* if $R = A \times B$. If R is a relation from A to B then the sets
$$D_R = \{a \in A : (a,b) \in R \text{ for some } b \in B\} \text{ and}$$
$$R_R = \{b \in B : (a,b) \in R \text{ for some } a \in A\}$$
are subsets of A and B and are called the *domain* and *range* of the relation R. R is clearly a subset of $D_R \times R_R$ but, in general, may not coincide with it.

For example, let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d, e, f\}$, then
$$R = \{(1, a), (1, b), (3, b), (4, f)\}$$
is a relation from A to B with
$$D_R = \{1, 3, 4\} \text{ and } R_R = \{a, b, f\}$$
Obviously, R in spite of being a subset of $A \times B$, is also a subset of $D_R \times R_R$.

1-2.4 Definition: If R is a relation in A, then the *complement of relation* R is denoted by R^c and is defined as $R^c = (A \times A) - R$. Thus $(a, b) \in R^c$ if and only if $(a, b) \notin R$.

1-2.5 Definition: A binary relation I is called the *identity relation* on A if
$$I = \{(a, a) : a \in A\}$$
For example,
$$I = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$$
is an identity relation on $A = \{1, 2, 3, 4, 5\}$.

1-2.6 Definition: The *inverse of a binary relation* R is a binary relation
$$R^{-1} = \{(b, a) : (a, b) \in R\}$$
For example, the inverse of the binary relation
$$R = \{(1, a), (2, b), (3, a)\}$$
is
$$R^{-1} = \{(a, 1), (b, 2), (a, 3)\}$$

A relation on a set A may or may not satisfy some specified conditions. Relations which do have certain additional properties are of relatively greater significance. A few of such relations are given in the following definitions.

1-2.7 Definition: A relation R on a set A is said to be the *reflexive relation* if R contains the identity relation I.

Thus R is reflexive if and only if

$$(a, a) \in R \text{ for all } a \in R$$

Let $A = \{1, 2, 3, 4, 5\}$, then

$R = \{(1,1), (1,2), (1,3), (2,2), (3, 3), (4, 4), (4, 5), (5, 1), (5, 2), (5, 3), (5, 4), (5,5)\}$ is reflexive, because R contains the identity relation.

1-2.8 Definition: A relation R on a set A is *symmetric* if and only if $R = R^{-1}$. Thus R is symmetric relation on A if and only if

$$(a, b) \in R \Rightarrow (b, a) \in R \text{ for all } a, b \in A$$

The relation

$$R = \{(1, 2), (2, 1), (1, 3), (3, 1), (3, 3)\}$$

is a symmetric relation on A.

1-2.9 Definition: The relation R on A is said to be a *transitive relation* if

$$(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R \text{ for all } a, b, c \in A$$

For example,

$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (1, 3), (3, 2), (3, 1), (2, 3), (3, 3)\}$ is a transitive relation.

1-2.10 Definition: The relation R on A is said to be *anti-symmetric relation* if $R \cap R^{-1} = I$.

Thus a relation R is anti-symmetric if

$$(a, b) \in R, (b, a) \in R \Rightarrow a = b \text{ for all } a, b \in A$$

Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 2), (2, 2), (3, 3)\}$, then

$$R^{-1} = \{(1, 1), (2, 1), (2, 2), (3, 3)\}$$

Obviously

$$R \cap R^{-1} = \{(1, 1), (2, 2), (3, 3)\} = I$$

Hence R is anti-symmetric relation.

1-2.11 Definition: A relation R on a set A is called an *equivalence relation* if and only if R is reflexive, symmetric, and transitive. The identity relation and the full relation on a set A are equivalence relations.

Equivalence relations on a set A are usually denoted by the symbol '~' (pronounced as 'tilde') rather than by R as a set of ordered pairs of elements of A. Thus if R is an equivalence relation on A and $(a, b) \in R$, then we shall write $a \sim b$. With this notation the definition of an equivalence relation becomes:

A relation '~' on a set A is an *equivalence relation* if and only if for all $a, b, c \in A$,

1. $a \sim a$ (reflexive)
2. $a \sim b \Rightarrow b \sim a$ (symmetric)
3. $a \sim b$ and $b \sim c \Rightarrow a \sim c$ (transitive)

1-2.12 Definition: If R is an equivalence relation on A, then the set of those elements of A which are related to a fixed element a of A under the relation R is called an *equivalence class* determined by the element a and is denoted by C_a. Thus,

$$C_a = \{b \in A : (a, b) \in R\}$$

For each $a \in A$, the equivalence class C_a is non-empty because, by the reflexive property of R, at least $(a, a) \in R$ and $a \in C_a$. The element a is called a *representative element* of C_a.

1-2.13 Definition: A collection $\{A_\alpha : A_\alpha \subseteq A, \alpha \in I\}$ of subsets of A is said to be the *partition* of A if

(i) $A_\alpha \cap A_\beta = \phi$ if $\alpha \neq \beta$

(ii) $\bigcup_{\alpha \in I} A_\alpha = A$

1-2.14 Theorem: *Each equivalence relation on a set A determines a partition of A.*

Proof: Suppose that R is an equivalence relation on A and $C = \{C_a : a \in A\}$ the collection of equivalence classes of A determined by R. Then each C_a is a subset of A, so

$$\cup C_a \subseteq A \quad \ldots(1)$$

As R is reflexive, the pair $(a, a) \in R$ for all $a \in A$. Hence every $a \in A$ is in an equivalence class namely the equivalence class determined by a. Thus $a \in \cup C_a$ for all $a \in A$. Hence

$$A \subset \cup C_a \quad (2)$$

From (1) and (2), we have

$$A = \cup C_a \quad (3)$$

Further let C_a, C_b be distinct equivalence classes in C. Let $C_a \cap C_b \neq \phi$ and let $x \in C_a \cap C_b$, then $x \in C_a$ and $x \in C_b$, i.e. $(a, x) \in R$ and $(b, x) \in R$. As R is symmetric, $(x, b) \in R$ and, by the transitivity of R, $(a, b) \in R$. This shows that $b \in C_a$.

Now let $y \in C_b$, then $(b, y) \in R$. Once again, by the transitivity of R, $(a, b) \in R$, $(b, y) \in R$ imply $(a, y) \in R$.

Thus $y \in C_a$. Hence $C_b \subset C_a$.

Similarly $C_a \subset C_b$. Hence $C_a = C_b$ which is a contradiction to our assumption that C_a and C_b are distinct. So, $C_a \cap C_b = \phi$.

This shows that $C = \{C_a : a \in A\}$ is a partition of A.

1-2.15 Example:
Show that $R = \{(0, 0), (1, 1), (2, 2), (3, 3), (0, 2), (1, 3), (2, 0), (3, 1)\}$ *is an equivalence relation in* $A = \{0, 1, 2, 3\}$.

Solution: The reflexive property holds, i.e. $(x, x) \in R$ for all $x \in A$, since $(0, 0), (1, 1), (2, 2), (3, 3) \in R$.

To show that R is symmetric, let us examine all pairs (x, y) where $x \neq y$. There are only four, namely

$$(0, 2), (1, 3), (2, 0), (3, 1)$$

Clearly if (x, y) is anyone of the four, so is (y, x).

When $x = y$, $(x, y) = (y, x)$. Thus $(x, y) \in R$ implies $(y, x) \in R$. R is also transitive. Let $(x, y) \in R$ and $(y, z) \in R$. Suppose $x \neq y$. Then (x, y) can be $(0, 2), (1, 3), (2, 0)$ or $(3, 1)$. If $(x, y) = (0, 2)$, then $(y, z) = (2, 0)$ or $(2, 2)$ and $(x, z) = (0, 0)$ or $(0, 2)$ respectively. Hence $(x, z) \in R$.

Similarly if $(x, y) = (1, 3), (2, 0)$ or $(3, 1)$, it can be shown that $(x, z) \in R$. When $x = y$, $(y, z) \in R$ means $(x, z) \in R$. Therefore for any $(x, y) \in R$ and $(y, z) \in R$, we have $(x, z) \in R$ and R is transitive.

1-3 Functions

In this section we shall give the definitions of functions and their different types with suitable examples will also be discussed in details.

1-3.1 Definition: Let X and Y be two non-empty sets. A rule f which assigns to each element x in X a single element y in Y is called a *function*. The element y which corresponds in this way to a given x is usually written $f(x)$, and is called the *image* of x under the rule f, or the value of f at the element x. The element x is called the *pre-image* of $f(x)$.

Algebraists often write mappings on the right; other mathematicians write them on the left. In fact, we shall not be absolutely consistent in this ourselves; when we shall want to emphasise the functional nature of f we may very well write $y = f(x)$.

The notion is supposed to be suggestive of the idea that the rule f takes the element x and does something to it to produce the element $y = f(x)$. The rule f is often called a *mapping* , or *transformation*, or *operator*, and is written as $f : X \to Y$. The sets X and Y may be equal or may be different.

The sets X and Y are called the *domain* and *codomain* respectively of the function f, and the set of all $f(x)$'s for all x's in X is called its *range*.

1-3.2 Definition: A function whose range consists of just one element is called a *constant function*. For example, the function f, defined as, $f(x) = 2 \forall x \in D_f$, where D_f is domain of f, is a constant function, because its range consists of a single element, i.e. 2.

1-3.3 Definition: A function f is called an *extension* of a function g if the domain of f contains the domain of g and $f(x)=g(x)$ for each x in the domain of g. In this case the function g is called the *restriction* of f. For example, if $D_f=\{1,2,3,...,100\}, D_g=\{4,8,12,...,50\}$ such that $f(x)=x^2$ and $g(x)=x^2$, then f is an extension of g and g is the restriction of f. As a matter of usage, we generally prefer to reserve the term *function* for real or complex functions and to speak of *mappings* when dealing with functions whose values are not necessarily numbers.

1-3.4 Definition: If the range, R_f, of a mapping $f:X\to Y$ is the set Y, then we call f a mapping of X *onto* Y. Such a mapping is also called the *surjective mapping*.

1-3.5 Definition: If different elements in X have different images in Y under $f:X\to Y$, then f is called *one-to-one mapping* of X into Y. Such a mapping is also called the *injective mapping*.

1-3.6 Definition: If a mapping $f:X\to Y$ is both one-to-one and onto, we call f a *one-to-one mapping* of X *onto* Y. Such a mapping is also called the *bijective mapping*.

A constant mapping is always an onto mapping, and the constant mapping with a single element in its domain is bijective. The bijective mappings are very useful in testing whether two sets have same number of elements or not.

1-3.7 Definition:

If $f:X\to Y$ is a bijective mapping, then we can find a rule $f^{-1}:Y\to X$ which assigns to each element y in Y a single element x in X. This rule is said to be the *inverse mapping*, and the image x of y under the inverse mapping is written as $f^{-1}(y)=x$, which is obtained by solving the equation $y=f(x)$ for x.

1-3.8 Example: *If $f:X\to Y$ is a bijective mapping defined as $y=f(x)=2x$, then find its inverse mapping.*

Solution: The inverse mapping $f^{-1}:Y\to X$ is defined as $x=\frac{1}{2}y$ or $f^{-1}(y)=x$ or $f^{-1}(2x)=x$.

1-3.9 Definition: The mappings f and g of X into Y are said to be *equal* if $f(x)=g(x)$ for every $x\in X$.

1-3.10 Definition: The *composition* or *product* of two mappings $f: X \to Y$ and $g: Y \to Z$ is the mapping $g \circ f: X \to Z$ defined by means of $g \circ f(x) = g(f(x))$ for every $x \in X$.

1-4 Binary Operations

In this section we shall discuss very important concepts which will be helpful in defining and understanding the group theory appearing in the next chapters.

1-4.1 Definition: The *binary operation* '$*$' in A is a rule which associates with every ordered pair (a, b), where $a, b \in A$, a uniquely determined element of the set A. This element is denoted by $a * b$. We can also define the binary operation as follows.

Any mapping $*$ of $X \times X$ into X, where X is any non-empty set, is called a *binary operation* in X. Thus the mapping $*: X \times X \to X$ is called the binary operation in X. The image of $(x, y) \in X \times X$ is denoted by $x * y \in X$. We write $*(x, y) = x * y$.

1-4.2 Definition: If a binary operation $*$ can be defined on a set A, then the set A is said to be *closed* under the binary operation $*$. This property of the set is called the *closure property*.

1-4.3 Example: Since the addition and multiplication of two integers is also an integer, so the set of all integers is closed under ordinary addition and multiplication.

Similarly, the set of natural numbers is also closed under addition and multiplication.

Since the difference of two natural numbers may not be a natural number, so, the set of all naturals is not closed under subtraction.

1-4.4 Definition: Let $*$ be a binary operation in a non-empty set X then an element $e \in X$ is said to be the *identity element* (with respect to $*$) of X if $e * x = x * e = x \; \forall x \in X$.

For example, 0 is the identity element of the set of integers with respect to + (addition) and 1 is the identity element of set natural numbers with respect to multiplication.

1-4.5 Definition: The *inverse* of an element $x \in X$ with respect to $*$ is an element $x' \in X$ such that $x * x' = e = x' * x$, where e is the identity element of X. In fact, x and x' are inverses of each other.

Thus the multiplicative and additive inverses of x are x^{-1} and $-x$ respectively.

1-4.6 Definition: A binary operation $*$ is said to satisfy the *associative law* in X if $x*(y*z)=(x*y)*z\ \forall x,y,z\in X$.

1-4.7 Definition: A binary operation $*$ is said to satisfy the *commutative law* in X if $x*y=y*x\ \forall x,y\in X$.

Addition and multiplication always satisfy the associative and multiplication laws.

1-4.8 Example:
Show that the mapping $*:(m,n)\to m+n$, *where* $m,n\in N$ *is a binary operation in N.*
Solution: Since for every $m,n\in N$, $m+n\in N$ is a unique element of N, so, $*$ is a binary operation in N.

EXERCISE 1

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) $A-B=$

(a) $\{x\in A: x\notin B\}$ (b) $\{x\in B: x\notin A\}$

(c) $\{x: x\in A$ and $x\in B\}$ (d) $\{x: x\in A$ or $x\in B\}$

ⓐ ⓑ ⓒ ⓓ

(ii) $(A\cup B)^c=$

(a) $A^c\cup B^c$ (b) $A^c\cap B^c$

(c) $A\cup B$ (d) $A\cap B$

ⓐ ⓑ ⓒ ⓓ

(iii) If $R=\{(1,a),(2,b),(3,a)\}$, then

(a) $R^{-1}=\{(a,1),(b,2)\}$ (b) $R^{-1}=\{(1,1),(2,2),(3,3)\}$

(c) $R^{-1}=\{(b,2),(a,3)\}$ (d) $R^{-1}=\{(a,1),(b,2),(a,3)\}$

ⓐ ⓑ ⓒ ⓓ

(iv) If $a\sim b$ and $b\sim c\Rightarrow a\sim c$, then $\sim$ is

(a) reflexive (b) symmetric

(c) transitive (d) none of these

ⓐ ⓑ ⓒ ⓓ

(v) A function whose range consists of just one element is called

(a) one-one function (b) identity function

(c) bijective function (d) constant function

ⓐ ⓑ ⓒ ⓓ

(vi) Which of the following is not a binary operation on N?
(a) + (b) × (c) ÷ (d) none of these
ⓐ ⓑ ⓒ ⓓ

(vii) $A \cap U =$
(a) U (b) A
(c) $\emptyset$ (d) A^c
ⓐ ⓑ ⓒ ⓓ

(viii) $A \cup \emptyset =$
(a) U (b) A
(c) $\emptyset$ (d) A^c
ⓐ ⓑ ⓒ ⓓ

(ix) $A \cup U =$
(a) U (b) A
(c) $\emptyset$ (d) A^c
ⓐ ⓑ ⓒ ⓓ

(x) $A \cap \emptyset =$
(a) U (b) A
(c) $\emptyset$ (d) A^c
ⓐ ⓑ ⓒ ⓓ

(xi) For a binary operation $*$ in Q defined as $a * b = 9ab$, the identity element with respect to $*$ is
(a) $\frac{1}{3}$ (b) $\frac{1}{9}$ (c) $\frac{1}{27}$ (d) $\frac{1}{81}$
ⓐ ⓑ ⓒ ⓓ

(xii) For a binary operation $*$ in Q defined as $a * b = 9ab$, the inverse of $\frac{1}{3}$ is
(a) $\frac{1}{3}$ (b) $\frac{1}{9}$ (c) $\frac{1}{27}$ (d) $\frac{1}{81}$
ⓐ ⓑ ⓒ ⓓ

(xiii) For a binary operation $*$ in Q defined as $a * b = \frac{1}{6}ab$, the inverse of 36 is
(a) $\frac{1}{36}$ (b) $\frac{1}{12}$ (c) $\frac{1}{6}$ (d) 1
ⓐ ⓑ ⓒ ⓓ

(xiv) For a binary operation $*$ in Q defined as $a * b = \int_0^{\sqrt{ab}} x\,dx$, the identity element with respect to $*$ is
(a) -2 (b) 0 (c) 1 (d) 2
ⓐ ⓑ ⓒ ⓓ

(xv) If a binary operation $*$ in Q is defined as $a * b = \int_0^{\sqrt{ab}} x dx$, then the inverse of $\frac{5}{9}$ with respect to $*$ is

(a) $\frac{9}{5}$ (b) $\frac{36}{5}$ (c) $\frac{38}{5}$ (d) 36

ⓐ ⓑ ⓒ ⓓ

(xvi) If a binary operation $*$ in Q is defined as $a * b = \int_0^{\sqrt{ab}} x dx$, then the inverse of $\frac{36}{5}$ with respect to $*$ is

(a) $\frac{9}{5}$ (b) $\frac{5}{36}$ (c) $\frac{5}{9}$ (d) 9

ⓐ ⓑ ⓒ ⓓ

(xvii) If a binary operation $*$ in Q is defined as $a * b = \begin{vmatrix} 3a & 1 \\ 0 & b \end{vmatrix}$, then the identity element with respect to $*$ is

(a) -2 (b) -1 (c) 0 (d) $\frac{1}{3}$

ⓐ ⓑ ⓒ ⓓ

(xviii) For a binary operation $*$ in Q defined as $a * b = \begin{vmatrix} 3a & 1 \\ 0 & b \end{vmatrix}$, the inverse of $\frac{1}{18}$ is

(a) -2 (b) -1 (c) 0 (d) $\frac{1}{3}$

ⓐ ⓑ ⓒ ⓓ

(xix) For a binary operation $*$ in Q defined as $a * b = \begin{vmatrix} 3a & 1 \\ 0 & b \end{vmatrix}$, the inverse of 2 is

(a) -2 (b) $\frac{1}{2}$ (c) 0 (d) $\frac{1}{18}$

ⓐ ⓑ ⓒ ⓓ

(xx) If $*$ is a binary operation in A then

(a) A is closed under $*$ (b) A is not closed under $*$

(c) A is closed under + (d) A is closed under −

ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.2 Solve / answer the following short questions:

(i) If $A \subseteq B$ and $B \subseteq C$, then show that $A \subseteq C$.

(ii) Show that $A \subseteq B$ if and only if $A \cap B = A$.

(iii) If $A \subseteq B$, then show that $(B - A) \cup A = B$.

(iv) Let A and B be sets. Show that $(A \cap B) \subseteq A$.

(v) Let A and B be sets. Show that $A \subseteq (A \cup B)$.

(vi) Let A and B be sets. Show that $A \cap (B - A) = \emptyset$.

(vii) Which of the following are binary operations in N?

(a) $*: (m,n) \to m - n$, where $m,n \in N$

(b) $*: (m,n) \to m \div n$, where $m,n \in N$

(c) $*: (m,n) \to mn$, where $m,n \in N$

(d) $*: (m,n) \to m$, where $m,n \in N$

(e) $*: (m,n) \to m + n + m^2$, where $m,n \in N$

(f) $*: (m,n) \to m + n - m^2$, where $m,n \in N$

(g) $*: (m,n) \to \frac{mn}{3}$, where $m,n \in N$

(h) $*: (m,n) \to \frac{m+n}{2}$, where $m,n \in N$

(viii) Which of the following binary operations are commutative?

(a) $m \circ n = m + n + mn$, where $m,n \in N$

(b) $m \circ n = m + n - mn$, where $m,n \in N$

(c) $m \circ n = m - n + mn$, where $m,n \in N$

(d) $a \circ b = \frac{a+b+ab}{2}$, where $a,b \in Q$

(e) $a \circ b = \frac{a+b-ab}{3}$, where $a,b \in Q$

(f) $a \circ b = \frac{a-b+ab}{4}$, where $a,b \in Q$

(g) $a \circ b = \frac{a+b}{3}$, where $a,b \in Q$

(h) $a \circ b = \frac{a-b}{3}$, where $a, b \in Q$

(ix) Let $\circ$ be the binary operation in R^2 defined by $(x,y) \circ (x',y') = (xx' - yy', yx' + xy')$ for all $(x,y), (x',y') \in R^2$. Show that $\circ$ is commutative binary operation.

Q.3 Solve / answer the following short questions:

(i) Define the binary operation in a set A.

(ii) Define a binary operation $*$ in Q as $a * b = 9ab$. Show that the commutative law holds in Q with respect to $*$.

(iii) Define a binary operation $*$ in Q as $a * b = 9ab$. Show that the associative law holds in Q with respect to $*$.

(iv) Define a binary operation $*$ in Q as $a * b = 9ab$. Show that $\frac{1}{9}$ is the identity element with respect to $*$.

(v) Define a binary operation $*$ in Q as $a * b = 9ab$. Show that $\frac{1}{27}$ is the inverse of $\frac{1}{3}$ with respect to $*$.

(vi) Define a binary operation $*$ in Q as $a * b = 9ab$. Find the inverse of 27 with respect to $*$.

(vii) Define a binary operation $*$ in Q as $a * b = \frac{1}{6}ab$. Find the inverse of 36 with respect to $*$.

(viii) Define a binary operation $*$ in Q as $a * b = \int_0^{\sqrt{ab}} x\,dx$. Find the identity element with respect to $*$.

(ix) Define a binary operation $*$ in Q as $a * b = \int_0^{\sqrt{ab}} x\,dx$. Find the Find the inverse of $\frac{5}{9}$ with respect to $*$.

(x) Define a binary operation $*$ in Q as $a * b = \begin{vmatrix} 3a & 1 \\ 0 & b \end{vmatrix}$. Find the identity element with respect to $*$.

(xi) Define a binary operation $*$ in Q as $a * b = \begin{vmatrix} 3a & 1 \\ 0 & b \end{vmatrix}$. Find the inverse of $\frac{1}{18}$ with respect to $*$.

Long Questions

Q.4 Show that $A - B = A \cap B^c$.

Q.5 Let A and B be subsets of a universal set U. Show that $A \subseteq B$ if and only if $B^c \subseteq A^c$.

Q.6 Prove that $(A \cup (B \cap C))^c = (C^c \cup B^c) \cap A^c$.

Q.7 Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

SUMMARY

- The collection of well defined objects is called a set. The well defined objects of this collection are said to be the elements or points of the set.
- A set can be expressed by descriptive statement and this way of expressing a set is called the descriptive method.
- If we list the elements of the set by writing them within braces, then this method of writing a set is said to be the tabular method. For example, the set of first ten positive even integers is written as $\{2, 4, 6, 8, 10\}$.
- If we describe a set by stating a characteristic property which identifies all the elements of the set then this method is said to be set builder method. For example,

  $A = \{x : x \text{ is an integer between 10 and 20}\}$

  $B = \{x : x \text{ is a BS student of GCS during 2014}\}$
- A set which contains no elements is called an empty set or vacuous set or null set. It is denoted by ϕ.
- A set A is said to be the subset of a set B if every element of A is also an element of B.
- If A is a subset of B and B has at least one element which is not in A, then A is called the proper subset of B.
- Two sets A and B are said to be equal if $A \subset B$ and $B \subset A$. In this case we write $A = B$. If there is at least one element of B which is not in A, then A is not equal to B and we write $A \neq B$.
- The difference $A - B$ of two sets A and B is defined to be set of those elements of A which are not in B.
- If $B \subset A$, then $A - B = \{x \in A : x \notin B\}$ is said to be the complement of B in A. This definition shows that the complement of a set A in

A is an empty set. The complement of a set A is usually denoted by A^c.

- The union of two sets A and B is a set whose elements are elements of A or of B.
- The intersection of two sets A and B, denoted by $A \cap B$, is a set whose elements are in both A and B.
- Two sets A and B are said to be disjoint if they have no common points.
- Given a set I, if for each $\alpha \in I$, there is a set A_α, then $\{A_\alpha : \alpha \in I\}$ is called an indexed family of sets and the set I is called the indexing set.
- If all the under consideration sets are assumed to be the subsets of a single fixed set then this fixed set is said to be universal set.
- Let A and B be two nonempty sets, then the set consisting of all ordered pairs (a, b), where $a \in A$ and $b \in B$, is called the Cartesian product of A and B and is denoted by $A \times B$.
- A subset R of $A \times B$ is called a binary relation or simply a relation from A to B.
- A relation R from A to B is said to be empty or nullary if $R = \phi$ and full if $R = A \times B$.
- If R is a relation in A, then the complement of relation R is denoted by R^c and is defined as $R^c = (A \times A) - R$. Thus $(a, b) \in R^c$ if and only if $(a, b) \notin R$.
- A binary relation I is called the identity relation on A if
$$I = \{(a, a) : a \in A\}$$
- The inverse of a binary relation R is a binary relation
$$R^{-1} = \{(b, a) : (a, b) \in R\}$$
- A relation R on a set A is said to be the reflexive relation if R contains the identity relation I.
- A relation R on a set A is symmetric if and only if $R = R^{-1}$. Thus R is symmetric relation on A if and only if $(a, b) \in R \Rightarrow (b, a) \in R$ for all $a, b \in A$.
- The relation R on A is said to be a transitive relation if $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ for all $a, b, c \in A$.
- Relation R on A is said to be anti-symmetric relation if $R \cap R^{-1} = I$.

- A relation R on a set A is called an equivalence relation if and only if R is reflexive, symmetric, and transitive.
- The identity relation and the full relation on a set A are equivalence relations.
- If R is an equivalence relation on A, then the set of those elements of A which are related to a fixed element a of A under the relation R is called an equivalence class determined by the element a and is denoted by C_a. Thus, $C_a = \{b \in A : (a, b) \in R\}$.
- A collection $\{A_\alpha : A_\alpha \subseteq A, \alpha \in I\}$ of subsets of A is said to be the partition of A if $A_\alpha \cap A_\beta = \phi$ for $\alpha \neq \beta$ and $\bigcup_{\alpha \in I} A_\alpha = A$.
- Each equivalence relation on a set A determines a partition of A.
- Let X and Y be two non-empty sets. A rule f which assigns to each element x in X a single element y in Y is called a function. The element y which corresponds in this way to a given x is usually written $f(x)$, and is called the image of x under the rule f, or the value of f at the element x. The element x is called the pre-image of $f(x)$.
- A function f is called an extension of a function g if the domain of f contains the domain of g and $f(x) = g(x)$ for each x in the domain of g. In this case the function g is called the restriction of f.
- A function whose range consists of just one element is called a constant function.
- If the range, R_f, of a mapping $f : X \to Y$ is the set Y, then we call f a mapping of X onto Y. Such a mapping is also called the surjective mapping.
- If different elements in X have different images in Y under $f : X \to Y$, then f is called one-to-one mapping of X into Y. Such a mapping is also called the injective mapping.
- If a mapping $f : X \to Y$ is both one-to-one and onto, we call f a one-to-one mapping of X onto Y. Such a mapping is also called the bijective mapping.
- If $f : X \to Y$ is a bijective mapping, then we can find a rule $f^{-1} : Y \to X$ which assigns to each element y in Y a single element x in X. This rule is said to be the inverse mapping, and the image x of y under the inverse mapping is written as $f^{-1}(y) = x$, which is obtained by solving the equation $y = f(x)$ for x.

- The mappings f and g of X into Y are said to be equal if $f(x) = g(x)$ for every $x \in X$.
- Any mapping $*$ of $X \times X$ into X, where X is any nonempty set, is called a binary operation in X.
- If a binary operation $*$ can be defined on a set A, then the set A is said to be closed under the binary operation $*$. This property of the set is called the closure property.
- Let $*$ be a binary operation in a nonempty set X then an element $e \in X$ is said to be the identity element (with respect to $*$) of X if $e * x = x * e = x \; \forall x \in X$.
- The inverse of an element $x \in X$ with respect to $*$ is an element $x' \in X$ such that $x * x' = e = x' * x$, where e is the identity element of X.
- A binary operation $*$ is said to satisfy the associative law in X if $x * (y * z) = (x * y) * z \; \forall x, y, z \in X$.
- A binary operation $*$ is said to satisfy the commutative law in X if $x * y = y * x \; \forall x, y \in X$.

*****

Chapter 2

GROUPS

The study of groups arose early in the nineteenth century. Originally a group was a set of permutations with the property that the combination of any two permutations again belongs to the set. Subsequently this definition was generalised to the concept of an abstract group, which was defined to be a set, not necessarily of permutations, together with a method of combining its elements that is subject to a few simple laws.

Group theory plays an important part in present day mathematics and science. Groups appear in quantum mechanics, geometry, topology, physics, chemistry and even in biology.

Although groups arose in connection with other disciplines, the study of groups is in itself exciting. Currently there is a vigorous research in the subject, and it attracts the energies and imagination of a great many mathematicians.

In this chapter we shall first give some definitions and then we shall give several examples of groups. The concepts of orders of elements of groups are discussed in the second section of this chapter. Cyclic groups and Lagrange's theorem are also discussed at the end.

2-1 Definition, Examples and Formation of Groups

In this section we shall define a group and we shall also give several examples of groups. Some basic concepts concerning to groups are also discussed in details. Keeping in mind the difficulties of students to understand the subject, the examples are solved in details.

2-1.1 Definition: Let G be a nonempty set. The ordered pair $(G,*)$ is said to be a *group* if it satisfies the following axioms:

G_1): $a*b \in G \quad \forall a,b \in G$ (closure property)

G_2): $a*(b*c)=(a*b)*c \ \forall a,b,c \in G$ (associative law)

G_3): For each $a \in G$, there exists an element $e \in G$, known as the *identity element*, such that

$$a*e=e*a=a$$

This is called the *identity law*.

G_4): For each $a \in G$, there exists an element $a' \in G$, known as the *inverse* of a, such that

$$a*a'=a'*a=e$$

This law is called the *inverse law*.

The first axiom of group shows that $*$ is a binary operation in G.

2-1.2 Definition: If the commutative law holds in a group, then such a group is called an *abelian group* or *commutative group*. Thus the group $(G,*)$ is said to be an *abelian group* or *commutative group* if

$$a*b=b*a \ \forall a,b \in G$$

A group which is not abelian is called a *non-abelian group*. The group $(G,+)$ is called the *group under addition* while the group $(G,\cdot)$ is known as *group under multiplication*.

2-1.3 Example: *Show that the set of integers is an abelian group under addition.*

Solution:

G_1): Since the sum of two integers is also an integer, therefore

$$m+n \in Z \ \forall m,n \in Z$$

G_2): Associative law under addition holds in integers, so

$$l+(m+n)=(l+m)+n \ \forall l,m,n \in Z$$

G_3): Additive identity, 0, is also an integer, so there exists

$0 \in Z$ such that $n+0=n=0+n \ \forall n \in Z$

G_4): The additive inverse of each integer is also an integer, so

$-n \in Z \ \forall n \in Z$ such that $n+(-n)=0=-n+n$

G_5): The commutativ e law under addition holds in integers, so

$$m+n=n+m \ \forall m,n \in Z$$

Hence $(Z,+)$ is an abelian group.

2-1.4 Example: *Show that the set of real numbers is an abelian group under addition.*

Solution: G_1): Since the sum of two real numbers is also a real number, therefore, $x+y \in R \ \forall x,y \in R$.

G_2): Associative law under addition holds in real numbers, so

$$x+(y+z)=(x+y)+z \quad \forall x,y,z \in R$$

G_3): Additive identity, 0, is also a real number, so there exists $0 \in R$ such that $x+0=x=0+x \quad \forall x \in R$

G_4): The additive inverse of each real number is also a real number, so $-x \in R \quad \forall x \in R$ such that $x+(-x)=0=-x+x$

G_5): The commutative law under addition holds in real numbers, so $x+y=y+x \quad \forall x,y \in R$

Hence $(R,+)$ is an abelian group.

2-1.5 Example: *Show that the set of rational numbers is an abelian group under addition.*

Solution: G_1): Since the sum of two rational numbers is also a rational number, therefore, $x+y \in Q \quad \forall x,y \in Q$.

G_2): Associative law under addition holds in rational numbers, so $x+(y+z)=(x+y)+z \quad \forall x,y,z \in Q$

G_3): Additive identity, 0, is also a rational number, so there exists $0 \in Q$ such that $x+0=x=0+x \quad \forall x \in Q$

G_4): Additive inverse of each rational number is also a rational number, so $-x \in Q \quad \forall x \in Q$ such that $x+(-x)=0=-x+x$

G_5): The commutative law under addition holds in rational numbers, so $x+y=y+x \quad \forall x,y \in Q$

Hence $(Q,+)$ is an abelian group.

2-1.6 Example: *Show that the set of complex numbers is an abelian group under addition.*

PU, 2014 (BS Math)

Solution: G_1): Since the sum of two complex numbers is also a complex number, therefore, $z_1+z_2 \in C \quad \forall z_1,z_2 \in C$.

G_2): Associative law under addition holds in complex numbers, so $z_1+(z_2+z_3)=(z_1+z_2)+z_3 \; \forall z_1,z_2,z_3 \in C$

G_3): Additive identity, 0, is also a complex number, so numbers, so $0 \in C$ such that $z+0=z=0+z \; \forall z \in C$

G_4): Additive inverse of each complex number is also a complex number, so $-z \in C \quad \forall z \in C$ such that $z+(-z)=0=-z+z$

G_5): The commutative law under addition holds in complex numbers, so $z_1+z_2=z_2+z_1 \quad \forall z_1,z_2 \in C$

Hence $(C,+)$ is an abelian group.

2-1.7 Example: *Show that the set of even integers is an abelian group under addition.*

Solution: G_1): Since the sum of two even integers is also an even integer, so $m+n \in E \ \forall m,n \in E$.

G_2): Associative law under addition holds in even integers, so

$$l+(m+n)=(l+m)+n \ \forall l,m,n \in E$$

G_3): Additive identity, 0, is also an even integer, so there exists

$0 \in E$ such that $n+0=n=0+n \ \forall n \in E$

G_4): The additive inverse of each even integer is also an even integer, so

$-n \in E \ \forall n \in E$ such that $n+(-n)=0=-n+n$

G_5): The commutativ e law under addition holds in even integers, so

$$m+n=n+m \ \forall m,n \in E$$

Hence $(E,+)$ is an abelian group.

2-1.8 Example: *Show that the set of non-zero real numbers is an abelian group under multiplication.*

Solution: Since the product of two non-zero real numbers is also a nonzero real number, so

G_1): $xy \in R-\{0\} \ \forall x,y \in R-\{0\}$

G_2): Associative law under multiplica tion holds in nonzero real numbers, so $x(yz)=(xy)z \ \forall x,y,z \in R-\{0\}$

G_3): Multiplica tive identity, 1, is also a nonzero real number, so there exists $1 \in R$ such that $x.1=x=1.x \ \forall x \in R-\{0\}$

G_4): The multiplica tive inverse of each non - zero real number is also a nonzero real number, so

$$\frac{1}{x} \in R-\{0\} \ \ \forall x \in R-\{0\} \text{ such that } x\left(\frac{1}{x}\right)=1=\left(\frac{1}{x}\right)x$$

G_5): The commutativ e law under multiplica tion holds in nonzero real numbers, so $xy=yx \ \ \forall x,y \in R-\{0\}$

Hence $(R-\{0\},.)$ is an abelian group.

2-1.8 Example: *Show that $G=\{1,\omega,\omega^2\}$, where ω is the cube root of unity, is an abelian group under multiplication.*

Solution: We write the elements of G along a row and along a column as shown in the table below indicating the binary operation in the top left corner. The column headed by a_j in the upper row is called the jth column and the row with a_i in the left column is referred to as the ith row.

The empty places are then filled in by writing the product of an element a_i in the ith row with the element a_j in the jth column in the ij position. Filling all the nine places in this way we have the required table.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Since ω is a cube root of unity, so $\omega^3 = 1$

All the five axioms of the abelian group are obviously satisfied, therefore G is an abelian group under multiplication.

2-1.9 Example: *Show that the set $C_4 = \{\pm 1, \pm i\}$ of all the fourth roots of unity is a group under the usual multiplication.*

Solution: The product table of elements of C_4 is given by

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

All the five axioms of the abelian group are obviously satisfied, therefore C_4 is an abelian group under multiplication.

2-1.10 Example: *Show that the set G of all non-singular matrices of order 2 is a non-abelian group under matrix multiplication.*

Solution: G_1): Since the product of two non-singular matrices of order two is also a non-singular matrix of order two, so

$$AB \in G \quad \forall A, B \in G$$

G_2): The associative law under multiplication holds in matrices, so

$$A(BC) = (AB)C \quad \forall A, B, C \in G$$

G_3): Since identity matrix of order two is also a non-singular matrix, so it will be in G. Thus

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$$

such that $AI_2 = A = I_2 A \ \forall A \in G$.

G_4): Since the inverse of a non-singular matrix of order two is also a matrix of order two, so it will be in G, i.e.

$A^{-1} \in G \forall A \in G$ such that $AA^{-1} = I = A^{-1}A$

Hence G, the set of all non-singular matrices of order two, is a group under matrix multiplication.

In general, matrices do not satisfy the commutative law under multiplication, G is not an abelian group.

2-1.11 Example: *Show that the set of all those complex numbers whose module are* 1 *is group under multiplication.*

Solution: Let $G = \{z : z \in C, |z| = 1\}$.

$G_1)$: Let $z_1, z_2 \in G$, then $|z_1| = 1$ and $|z_2| = 1$.

Now $|z_1 z_2| = |z_1||z_2| = 1 \Rightarrow z_1 z_2 \in G$.

$G_2)$: Associative law holds in complex numbers.

$G_3)$: $1 \in G$ such that $1.z = z.1 = z \ \forall z \in G$.

$G_4)$: Let $z \in G$, then $|z| = 1$. Now $|z^{-1}| = \left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$.

Hence $z^{-1} \in G \ \forall z \in G$.

This show sthat $(G, .)$ is a group.

2-1.12 Example: *Show that the set of all irrational numbers is not a group under multiplication.*

Solution: Since the product of two irrational numbers is a rational number, so the set of irrational numbers is not closed under multiplication. Hence the set of irrational numbers is not a group under multiplication.

2-1.13 Example: *Show that the set of matrices*

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

forms a group under matrix multiplication.

Solution: Let $G = \{I, A, B, C\}$, then

$G_1)$:

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$$

$$BA = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$$

$$BC = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A$$

$$CB = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A$$

$$AC = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = B$$

$$CA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = B$$

$$A^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$B^2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$C^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

This shows that G is closed under matrix multiplication.

G_2): Associative law under multiplication holds in matrices, so it will also hold in G.

G_3): $AI = IA = A, BI = IB = B, CI = IC = C$

G_4): $A^2 = I \Rightarrow A^{-1} = A$, | $B^2 = I \Rightarrow B^{-1} = B$, | $C^2 = I \Rightarrow C^{-1} = C$

Hence G is a group under matrix multiplication.

2-1.14 Example:

Show that $G = \{2^k : k \in Z\}$ is a group under multiplication.

Solution: G_1): Let $x, y \in G$, then $x = 2^k, y = 2^l, k, l \in Z$.

Now $xy = 2^k 2^l = 2^{k+l} \in G \quad \because k + l \in Z$

G_2): Let $x, y, z \in Z$, then $x = 2^k, y = 2^l, z = 2^m, k, l, m \in Z$

$\Rightarrow x(yz) = 2^k(2^l 2^m)$

$= 2^k(2^{l+m}) = 2^{k+l+m}$

$= (2^k 2^l)2^m = (xy)z$

G_3): $1 = 2^0 \in G$

G_4): $2^{-k} \in G \ \forall 2^k \in G \quad (\because k \in Z \Rightarrow -k \in Z)$

Hence G is a group under multiplication.

2-1.15 Example: *Show that*

$$G = \{a + b\sqrt{2} : a, b \in Q, \text{either } a \neq 0 \text{ or } b \neq 0\}$$

is a group under multiplication.

Solution: G_1): Let $x, y \in G$, then $x = a + b\sqrt{2}, y = c + d\sqrt{2}$

$\Rightarrow xy = (a + b\sqrt{2})(c + d\sqrt{2}) = [(ac + 2bd) + (bc + ad)\sqrt{2}] \in G$

G_2): $x(yz) = (xy)z \ \forall x, y, z \in G$

G_3): $1 = (1 + 0\sqrt{2}) \in G$

G_4): $x^{-1} = \dfrac{1}{a + b\sqrt{2}} = \dfrac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2}$

$= \left[a(a^2 - 2b^2)^{-1} + b(2b^2 - a^2)^{-1}\sqrt{2}\right] \in G$

2-1.16 Example: *Show that*

$G = \{a + b\sqrt{-5} : a, b \in Q$, either $a \neq 0$ or $b \neq 0\}$

is a group under multiplication.

Solution: G_1): $x, y \in G \Rightarrow x = a + b\sqrt{-5}, y = c + d\sqrt{-5}$

$\Rightarrow xy = (a + b\sqrt{-5})(c + d\sqrt{-5})$

$= \left[(ac + 5bd) + (bc + ad)\sqrt{-5}\right] \in G$

G_2): $x(yz) = (xy)z \ \forall x, y, z \in G$

G_3): $1 = (1 + 0\sqrt{-5}) \in G$

G_4): $x^{-1} = \dfrac{1}{a + b\sqrt{-5}} = \dfrac{a - b\sqrt{-5}}{(a + b\sqrt{-5})(a - b\sqrt{-5})}$

$= \dfrac{a - b\sqrt{-5}}{a^2 - 25b^2} = \left[\dfrac{a}{a^2 - 5b^2} + \dfrac{-b}{a^2 - 5b^2}\sqrt{-5}\right] \in G$

This shows that G is a group under multiplication.

2-1.17 Example: *Show that the set* $G = \{0\hat{i} + y\hat{j} : y \in R\}$ *of vectors in a plane is an abelian group under vector addition.*

Solution:

G_1): $\vec{a}, \vec{b} \in G$

$\Rightarrow \vec{a} = 0\hat{i} + y_1\hat{j}, \vec{b} = 0\hat{i} + y_2\hat{j}, y_1, y_2 \in R$

$\Rightarrow \vec{a} + \vec{b} = \left[0\hat{i} + (y_1 + y_2)\hat{j}\right] \in G \because (y_1 + y_2) \in R$

G_2): Associative law holds in vector addition.

G_3): $0 = (0\hat{i} + 0\hat{j}) \in G$

G_4): $-\vec{a} = (0\hat{i} - y\hat{j}) \in G \ \forall \vec{a} \in G$

G_5): $\vec{a} + \vec{b} = \vec{b} + \vec{a} \quad \forall \vec{a}, \vec{b} \in G$

Hence G is an abelian group under vector addition.

2-1.18 Example:

Show that the set $G = \{x\hat{i} + 0\hat{j} : y \in R\}$ *of vectors in a plane is an abelian group under vector addition.*

Solution:

$G_1)$: $\vec{a},\vec{b} \in G$

$\Rightarrow \vec{a} = x_1\hat{i} + 0\hat{j}, \vec{b} = x_2\hat{i} + 0\hat{j}, x_1, x_2 \in R$

$\Rightarrow \vec{a} + \vec{b} = \left[(x_1 + x_2)\hat{i} + 0\hat{j}\right] \in G \because (x_1 + x_2) \in R$

$G_2)$: Associative law holds in vector addition.

$G_3)$: $0 = (0\hat{i} + 0\hat{j}) \in G$

$G_4)$: $-\vec{a} = (-x\hat{i} + 0\hat{j}) \in G \forall \vec{a} \in G$

$G_5)$: $\vec{a} + \vec{b} = \vec{b} + \vec{a} \quad \forall \vec{a},\vec{b} \in G$

Hence G is an abelian group under vector addition.

2-1.19 Example: *Show that the set* $G = \{x\hat{i} + y\hat{j} : x, y \in R\}$ *of vectors in a plane is an abelian group under vector addition.*

Solution:

$G_1)$: $\vec{a},\vec{b} \in G$

$\Rightarrow \vec{a} = x_1\hat{i} + y_1\hat{j}, \vec{b} = x_2\hat{i} + y_2\hat{j}, x_1, x_2, y_1, y_2 \in R$

$\Rightarrow \vec{a} + \vec{b} = \left[(x_1 + x_2)\hat{i} + (y_1 + y_2)\hat{j}\right] \in G$

$\because (x_1 + x_2), (y_1 + y_2) \in R$

$G_2)$: Associative law holds in vector addition.

$G_3)$: $0 = (0\hat{i} + 0\hat{j}) \in G$

$G_4)$: $-\vec{a} = -(x\hat{i} + y\hat{j}) = (-x\hat{i} - y\hat{j}) \in G \forall \vec{a} \in G$

$G_5)$: $\vec{a} + \vec{b} = \vec{b} + \vec{a} \quad \forall \vec{a},\vec{b} \in G$

Hence G is an abelian group under vector addition.

2-1.20 Example: *Show that the set of all non-singular upper triangular matrices of order two forms a non-abelian group under matrix multiplication.*

Solution:

Let $G = \left\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in R, a \neq 0, c \neq 0\right\}$ be the set of all non-singular upper triangular matrices of order two.

$G_1)$: Let $A,B \in G$, then $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, $a \neq 0, c \neq 0, x \neq 0, z \neq 0$

$$AB = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} ax & ay + bz \\ 0 & cz \end{bmatrix} \in G$$

$G_2)$: Associative law under multiplica tion holds in matrices.

$G_3): I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$

$G_4)$: Since the inverse of an upper triangular matrix is also an upper triangular matrix, so the inverse of each element of G is in G.

$G_5)$: In general, commutative law under multiplication does not hold in matrices, so G is non-abelian group under matrix multiplication.

2-1.21 Example: *Show that the set of all non-singular lower triangular matrices of order two forms a non-abelian group under matrix multiplication.*

Solution:

Let $G = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} : a,b,c \in R, a \neq 0, c \neq 0 \right\}$ be the set of all non-singular lower triangular matrices of order two.

$G_1)$: Let $A,B \in G$, then

$$A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}, B = \begin{bmatrix} x & 0 \\ y & z \end{bmatrix}, a \neq 0, c \neq 0, x \neq 0, z \neq 0$$

$$AB = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}\begin{bmatrix} x & 0 \\ y & z \end{bmatrix} = \begin{bmatrix} ax & 0 \\ bx+cy & cz \end{bmatrix} \in G$$

$G_2)$: Associative law under multiplica tion holds in matrices.

$G_3)$: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$

$G_4)$: Since the inverse of a lower triangular matrix is also a lower triangular matrix, so the inverse of each element of G is in G.

$G_5)$: In general, commutative law under multiplication does not hold in matrices, so G is non-abelian group under matrix multiplication.

2-1.22 Example:

Show that the set $G = \left\{ \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} : x \in R - \{0\} \right\}$ *of matrices of order two forms an abelian group under matrix multiplication.*

Solution: $G_1)$: Let $A,B \in G$, then

$$A = \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix}, x \neq 0, y \neq 0$$

$$AB = \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix}\begin{bmatrix} y & y \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & xy \\ 0 & 0 \end{bmatrix} \in G$$

$G_2)$: Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix} \in G$ such that

$$\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}=\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}$$

G_4): $\begin{bmatrix}1/x & 1/x\\ 0 & 0\end{bmatrix} \in G \forall \begin{bmatrix}x & x\\ 0 & 0\end{bmatrix} \in G$ such that

$$\begin{bmatrix}1/x & 1/x\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}=\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}=\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}\begin{bmatrix}1/x & 1/x\\ 0 & 0\end{bmatrix}$$

G_5): $$\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}\begin{bmatrix}y & y\\ 0 & 0\end{bmatrix}=\begin{bmatrix}xy & xy\\ 0 & 0\end{bmatrix}=\begin{bmatrix}yx & yx\\ 0 & 0\end{bmatrix}=\begin{bmatrix}y & y\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & x\\ 0 & 0\end{bmatrix}$$

This shows that G is an abelian group under matrix multiplication.

2-1.23 Example:

Show that the set $G=\left\{\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}: x \in R-\{0\}\right\}$ *of matrices of order two forms an abelian group under matrix multiplication.*

Solution: G_1): Let $A,B \in G$, then

$$A=\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}, B=\begin{bmatrix}y & 0\\ 0 & 0\end{bmatrix}, x \neq 0, y \neq 0$$

$$AB=\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}y & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}xy & 0\\ 0 & 0\end{bmatrix} \in G$$

G_2): Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} \in G$ such that

$$\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}$$

G_4): $\begin{bmatrix}1/x & 0\\ 0 & 0\end{bmatrix} \in G \ \forall \begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix} \in G$ such that

$$\begin{bmatrix}1/x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}1/x & 0\\ 0 & 0\end{bmatrix}$$

G_5): $$\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}y & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}xy & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}yx & 0\\ 0 & 0\end{bmatrix}=\begin{bmatrix}y & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}$$

This shows that G is an abelian group under matrix multiplication.

2-1.24 Example: *Show that the set*

$$G=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}: a,b,c,d\in R, ad-bc\neq 0\right\}$$

of matrices of order two forms a non-abelian group under matrix multiplication.

Solution: G_1): Let $A,B\in G$, then

$$A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}, B=\begin{bmatrix}w & x\\ y & z\end{bmatrix}, ad-bc\neq 0, wz-xy\neq 0$$

$$\Rightarrow AB=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}w & x\\ y & z\end{bmatrix}=\begin{bmatrix}aw+by & ax+bz\\ cw+dy & cx+dz\end{bmatrix}$$

Now $(aw+by)(cx+dz)-(ax+bz)(cw+dy)$

$$=(ad-bc)(wz-xy)$$

$$\neq 0 \quad \because ad-bc\neq 0 \text{ and } wz-xy\neq 0$$

$$\Rightarrow AB\in G \;\forall A,B\in G$$

G_2): Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\in G$ such that

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}$$

G_4): Let $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in G$, then $ad-bc\neq 0$

Now $A^{-1}=\begin{bmatrix}\frac{d}{ad-bc} & \frac{-b}{ad-bc}\\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}\end{bmatrix}$

$$\because \left(\frac{d}{ad-bc}\right)\left(\frac{a}{ad-bc}\right)-\left(\frac{-b}{ad-bc}\right)\left(\frac{-c}{ad-bc}\right)=ad-bc\neq 0$$

$$\therefore A^{-1}\in G \qquad \forall A\in G$$

This shows that G is a group under matrix multiplication. In general, the commutative law under multiplication does not hold in matrices, so G is non-abelian group under matrix multiplication.

2-1.25 Example:

Show that the set $G=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}: a,b,c,d\in R, ad-bc=1\right\}$ *of matrices of order two forms a non-abelian group under matrix multiplication.*

Solution: G_1): Let $A,B \in G$, then

$$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}, B=\begin{bmatrix} w & x \\ y & z \end{bmatrix}, \quad ad-bc=1,\ wz-xy=1$$

$$\Rightarrow AB=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix}=\begin{bmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{bmatrix}$$

Now $(aw+by)(cx+dz)-(ax+bz)(cw+dy)$

$$=(ad-bc)(wz-xy)$$

$$=1 \qquad \because ad-bc=1 \text{ and } wz-xy=1$$

$$\Rightarrow AB \in G \ \forall A,B \in G$$

G_2): Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

G_4): Let $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, then $ad-bc=1$

$$\text{Now } A^{-1}=\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}=\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in G$$

$$\Rightarrow A^{-1} \in G \ \forall A \in G$$

This shows that G is a group under matrix multiplication. In general, the commutative law under multiplication does not hold in matrices, so G is non-abelian group under matrix multiplication.

2-1.26 Example: *Show that the set*

$$G=\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b \in R, a^2+b^2 \neq 0\right\}$$

of matrices of order two forms an abelian group under matrix multiplication.

Solution: G_1): Let $A,B \in G$, then

$$A=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, B=\begin{bmatrix} c & d \\ -d & c \end{bmatrix}, a^2+b^2=1, c^2+d^2=1$$

$$\Rightarrow AB=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}=\begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}$$

Now $(ac-bd)^2+(ad+bc)^2=(a^2+b^2)(c^2+d^2)=1$

$\Rightarrow AB \in G \forall A,B \in G$

G_2): Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

G_4): Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$, then $a^2 + b^2 = 1$

$$\text{Now } A^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in G$$

$\Rightarrow A^{-1} \in G \forall A \in G$

G_5): $$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & bc+ad \\ -(bc+ad) & ac-bd \end{bmatrix}$$

$$BA = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ac-bd & bc+ad \\ -(bc+ad) & ac-bd \end{bmatrix}$$

$\Rightarrow AB = BA \ \forall A,B \in G$

This shows that G is an abelian group under matrix multiplication.

2-1.27 Example: *Show that the set*

$$G = \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} : a \in R, a \neq 0 \right\}$$

of matrices of order two forms an abelian group under matrix multiplication.

Solution: G_1): Let $A,B \in G$, then

$$A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, B = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}, a \neq 0, b \neq 0$$

$$\Rightarrow AB = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & a^{-1}b^{-1} \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & (ab)^{-1} \end{bmatrix}$$

$\because a \neq 0, b \neq 0 \therefore ab \neq 0$

$\Rightarrow AB \in G \qquad \forall A,B \in G$

G_2): Associative law under multiplica tion holds in matrices.

G_3): $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$$

G_4): Let $A = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \in G$, then $A^{-1} = \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \in G$

$\Rightarrow A^{-1} \in G \; \forall A \in G$

G_5): $AB = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & a^{-1}b^{-1} \end{bmatrix}$

$$= \begin{bmatrix} ab & 0 \\ 0 & (ab)^{-1} \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & (ba)^{-1} \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = BA$$

$\Rightarrow AB = BA \quad \forall A, B \in G$

This shows that G is an abelian group under matrix multiplication.

2-1.28 Example: *Let $(G,*)$ and $(G',\circ)$ be two groups. Prove that the set $G \times G' = \{(a,a') : a \in G, a' \in G'\}$ forms a group under the multiplication defined by*

$$(a_1,a_1') \bullet (a_2,a_2') = (a_1 * a_2, a_1' \circ a_2') \forall (a_1,a_1'),(a_2,a_2') \in G \times G'$$

Solution:

G_1): Since $(G,*)$ and $(G',\circ)$ are groups, so $a_1 * a_2 \in G$,

$a_1' \circ a_2' \in G' \; \forall a_1, a_2 \in G, a_1', a_2' \in G'$

$\Rightarrow (a_1 * a_2, a_1' \circ a_2') \in G \times G'$

$\Rightarrow (a_1,a_1') \bullet (a_2,a_2') \in G \times G' \; \forall (a_1,a_1'),(a_2,a_2') \in G \times G'$

G_2): Let $x, y, z \in G \times G'$, then $x = (a_1,a_1'), y = (a_2,a_2')$,

$z = (a_3,a_3')$, where $a_1, a_2, a_3 \in G, a_1', a_2', a_3' \in G'$.

Now $x \bullet [y \bullet z] = (a_1,a_1') \bullet [(a_2,a_2') \bullet (a_3,a_3')]$

$= (a_1,a_1') \bullet (a_2 * a_3, a_2' \circ a_3')$

$= (a_1 * (a_2 * a_3), a_1' \circ (a_2' \circ a_3'))$

$= ((a_1 * a_2) * a_3), (a_1' \circ a_2') \circ a_3')$

$= (a_1 * a_2, a_1' \circ a_2') \bullet (a_3,a_3')$

$= [(a_1,a_1') \bullet (a_2,a_2')] \bullet (a_3,a_3')$

$= [x \bullet y] \bullet z$

$\Rightarrow x \bullet [y \bullet z] = [x \bullet y] \bullet z \; \forall x, y, z \in G \times G'$

G_3): Let $(a,a') \in G \times G'$, and e, e' be the identities of G, G'

then $(a,a') \bullet (e,e') = (a * e, a' \circ e') = (a,a')$

and $(e,e') \bullet (a,a') = (e * a, e' \circ a') = (a,a')$

This show sthat (e,e') is an identity element of $G \times G'$.

G_4): If b, b' are inverses of a, a' respectively,
then $(a,a')\bullet(b,b') = (a*b, a'\circ b') = (e,e')$
and $(b,b')\bullet(a,a') = (b*a, b'\circ a') = (e,e')$
This show sthat $(b,b') \in G\times G'$ is the inverse of (a,a').
Hence the inverse of each element of $G\times G'$ is in $G\times G'$.
This show sthat $(G\times G',\bullet)$ is a group.

2-1.29 Example: *Show that the set*

$$G = \{a + b\sqrt{2} + c\sqrt{3} : a,b,c \in Q, \text{ either } a \neq 0 \text{ or } b \neq 0 \text{ or } c \neq 0\}$$

is not a group under multiplication

Solution: G_1): Let $x, y \in G$, then $x = a_1 + b_1\sqrt{2} + c_1\sqrt{3}$

and $y = a_2 + b_2\sqrt{2} + c_2\sqrt{3}$

$$\Rightarrow xy = (a_1 + b_1\sqrt{2} + c_1\sqrt{3})(a_2 + b_2\sqrt{2} + c_2\sqrt{3})$$

$$= a_1a_2 + 2b_1b_2 + 3c_1c_2 + (a_1b_2 + b_1a_2 + b_1c_2\sqrt{3} + b_2c_1\sqrt{3})\sqrt{2}$$

$$+ (a_1c_2 + a_2c_1)\sqrt{3}$$

Since $a_1b_2 + b_1a_2 + b_1c_2\sqrt{3} + b_2c_1\sqrt{3}$ is not rational in general due to irrational $\sqrt{3}$, so G is not closed under multiplica tion.
This shows that G is not a group under multiplication.

2-1.30 Example: *Show that the set* $G = \{a_\circ, a_1, ..., a_6\}$ *is an abelian group under the multiplication defined as*

$$a_i.a_j = \begin{cases} a_{i+j} & \text{if } i+j < 7 \\ a_{i+j-7} & \text{if } i+j \geq 7 \end{cases}$$

Solution: G_1): By the given definition of the product it is clear that the set G is closed under that particular product.

G_2): Associative law also holds in G.

G_3): $a_\circ.a_i = a_{\circ+i} = a_i = a_{\circ+i} = a_i.a_\circ \; \forall a_i \in G$.
This show sthat $a_\circ$ is an identity element of G.

G_4): $a_i.a_j = a_\circ = a_j.a_i$ if $i+j = 7$
This show sthat the inverse of each element of G is also in G.

G_5): $a_i.a_j = a_{i+j} = a_{j+i} = a_j.a_i$ if $i+j < 7$

$a_i.a_j = a_{i+j-7} = a_{j+i-7} = a_j.a_i$ if $i+j \geq 7$

This show sthat the commutativ e law holds in G.
Hence G is an abelian group under the given product.

2-1.31 Example: *Show that the set* $G=\{a_0,a_1,\ldots,a_{n-1}\}$ *is an abelian group under the multiplication defined as*

$$a_i.a_j=\begin{cases}a_{i+j} & \text{if } i+j<n\\ a_{i+j-n} & \text{if } i+j\geq n\end{cases}$$

Solution:

G_1): By the given definition of the product it is clear that the set G is closed under that particular product.

G_2): Associative law also holds in G.

G_3): $a_0.a_i=a_{0+i}=a_i=a_{0+i}=a_i.a_0\ \forall a_i\in G$.

This show sthat a_0 is an identity element of G.

G_4): $a_i.a_j=a_0=a_j.a_i$ if $i+j=n$

This show sthat the inverse of each element of G is also in G.

G_5): $a_i.a_j=a_{i+j}=a_{j+i}=a_j.a_i$ if $i+j<n$

$a_i.a_j=a_{i+j-n}=a_{j+i-n}=a_j.a_i$ if $i+j\geq n$

This show sthat the commutativ e law holds in G.

Hence G is an abelian group under the given product.

2-1.32 Example:

Let $G=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ *be the set of residue classes modulo* 5 *such that* $\bar{a}+\bar{b}=\bar{r}\ \forall\bar{a},\bar{b}\in G$, *where* $\bar{r}$ *is the remainder obtained after division of* $a+b$ *by* 5. *Show that* $(G,+)$ *is an abelian group.*

Solution: The sum of elements of G is shown by the table

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

G_1): This table shows that G is closed under addition.

G_2): The associative law also holds in G.

G_3): The identity element $\bar{0}$ belongs to G.

G_4): The table shows that the inverse of each element of G is also in G.

G_5): The commutative law under addition also holds in G.

Hence G is an abelian group under addition.

2-1.33 Example: *Let $G=\{\bar{1},\bar{2},\bar{3},\bar{4}\}$ be the set of nonzero residue classes modulo 5 such that $\bar{a}\cdot\bar{b}=\bar{r}\ \forall \bar{a},\bar{b}\in G$, where $\bar{r}$ is the remainder obtained after division of $a\cdot b$ by 5. Show that $(G,\cdot)$ is an abelian group.*

Solution: The sum of elements of G is shown by the table

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

G_1): This table shows that G is closed under multiplication.

G_2): The associative law also holds in G.

G_3): The identity element $\bar{1}$ belongs to G.

G_4): The table shows that the inverse of each element of G is also in G.

G_5): The commutative law under multiplication also holds in G.

Hence G is an abelian group under multiplication.

2-1.34 Example: *Let $G=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$ be the set of nonzero residue classes modulo 8 such that $\bar{a}\cdot\bar{b}=\bar{r}\ \forall \bar{a},\bar{b}\in G$, where $\bar{r}$ is the remainder obtained after division of $a\cdot b$ by 8. Show that $(G,\cdot)$ is an abelian group.*

PU, 2014 (BS Math)

Solution: The sum of elements of G is shown by the table

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

G_1): This table shows that G is closed under multiplication.

G_2): The associative law also holds in G.

G_3): The identity element $\bar{1}$ belongs to G.

G_4): The table shows that the inverse of each element of G is also in G.

G_5): The commutative law under multiplication also holds in G.

Hence G is an abelian group under multiplication.

2-1.35 Example: *Let $G=\{\bar{1},\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}\}$ be the set of nonzero residue*

classes modulo 9 such that $\bar{a}\cdot\bar{b}=\bar{r}\ \forall \bar{a},\bar{b}\in G$, *where* $\bar{r}$ *is the remainder obtained after division of* $a\cdot b$ *by* 9. *Show that* $(G,\cdot)$ *is an abelian group.*

Solution: The sum of elements of G is shown by the table

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{7}$	$\bar{2}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{7}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{1}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

G_1): This table shows that G is closed under multiplication.

G_2): The associative law also holds in G.

G_3): The identity element $\bar{1}$ belongs to G.

G_4): The table also shows that the inverse of each element of G is in G.

G_5): The commutative law under multiplication also holds in G.

Hence G is an abelian group under multiplication.

2-1.36 Example: *Show that the set* $G=\{\pm 1,\pm i,\pm j,\pm k\}$ *where*

$$ij=k,jk=i,ki=j,ji=-k,kj=-i,ik=-j,i^2=j^2=k^2=-1$$

is a non-abelian group under this multiplication of symbols.

Solution: Since all the axioms of the group are satisfied under the given multiplication of symbols, so G is a group.

Since $ij=k\neq -k=ji$, so G is a non-abelian group.

2-1.37 Example: *Show that the set of all n, nth roots of unity forms a group under the multiplication of complex numbers.*

Solution: Let $G=\{1,\omega,\omega^2,...,\omega^{n-1}\}$ be the set of all n, nth roots of unity, then $\omega=e^{\frac{2i\pi}{n}}$. Since all the axioms of an abelian group are satisfied, so G is an abelian group under the multiplication of complex numbers.

2-1.38 Theorem: *For any three elements a, b, c of a group G,*

1. $ab=ac\Rightarrow b=c$ *(Left Cancellation Law)*
2. $ba=ca\Rightarrow b=c$ *(Right Cancellation Law)*

Proof: Since G is a group, so $a\in G\Rightarrow a^{-1}\in G$.

1. $ab=ac\Rightarrow a^{-1}(ab)=a^{-1}(ac)\Rightarrow (a^{-1}a)b=(a^{-1}a)c$

$\Rightarrow eb=ec\Rightarrow b=c$

2. $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1} \Rightarrow b(aa^{-1}) = c(aa^{-1})$
$\Rightarrow be = ce \Rightarrow b = c$

2-1.39 Definition: If G is a non-empty set then the order pair $(G,*)$ is said to be *semi group* if

G_1): $a*b \in G \quad \forall a,b \in G$

G_2): $a*(b*c) = (a*b)*c \quad \forall a,b,c \in G$

2-1.40 Example: *Is $(Q,\circ)$ a semi group? Where Q is the set of rational numbers and $\circ$ is defined in Q as $a \circ b = a+b-ab$. Find the identity element if it exists.*

Solution: G_1): Since $a+b-ab \in Q \quad \forall a,b \in Q$, therefore
$a \circ b \in Q \quad \forall a,b \in Q$

G_2): Let $a,b,c \in Q$, then
$a \circ (b \circ c) = a \circ (b+c-bc) = a+(b+c-bc)-a(b+c-bc)$
$(a \circ b) \circ c = (a+b-ab) \circ c = (a+b-ab)+c-(a+b-ab)c$
$\Rightarrow a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a,b,c \in Q$
This show sthat $(Q,\circ)$ is a semi group.

G_3): Since $a \circ 0 = a+0-a(0) = a = 0+a-(0)a = 0 \circ a \forall a \in Q$
Hence 0 is the identity element of Q w ithrespect to $\circ$.

2-1.41 Example:
Is $(Z,\circ)$ a group? Where $\circ$ is defined by $a \circ b = 0 \quad \forall a,b \in Z$

Solution: Obviously Z is closed under $\circ$ but the identity element with respect to $\circ$ does not exist, so $(Z,\circ)$ is not a group. However, $(Z,\circ)$ is a semi group, because the associative law holds under the binary operation $\circ$.

2-1.42 Theorem: *In a group G, the identity element is unique.*

Proof: Let, if possible, e and f be two identities of G, then taking e as identity, we have

$$ef = f = fe \qquad ...(1)$$

Similarly, taking f as identity, we get

$$ef = e = fe \qquad ...(2)$$

Comparing (1) and (2), we have

$$e = f$$

This shows that the identity element in a group is unique.

2-1.43 Theorem: *In a group G, the inverse of each element is unique.*

Proof: Let, if possible, b and c be two inverses of an element $a \in G$, then

$$ab = e = ba \qquad ...(1)$$

and

$$ac = e = ca \qquad \ldots(2)$$

$$(1) \Rightarrow c(ab) = ce$$

$$\Rightarrow (ca)b = c$$

$$\Rightarrow eb = c \qquad \text{(using (2))}$$

$$\Rightarrow b = c$$

This shows that the inverse of each element of a group is unique.

2-1.44 Example: *Define a binary operation $*$ in Q as $a * b = 9ab$. Show that the commutative and the associative laws hold in Q with respect to $*$. Also show that $\frac{1}{9}$ is the identity element with respect to $*$ and $\frac{1}{27}$ is the inverse of $\frac{1}{3}$ with respect to $*$.*

Solution: $\because a * b = 9ab = 9ba = b * a \; \forall a, b \in Q$.

This shows that the commutative law holds in Q.

Now

$$a * (b * c) = a * (9bc) = 9a(9bc) = 9(9ab)c$$

$$= 9(a * b)c = (a * b) * c$$

This shows that the associative law holds in Q.

Since

$$a * \frac{1}{9} = 9a\frac{1}{9} = a = 9\frac{1}{9}a = \frac{1}{9} * a \quad \forall a \in Q$$

so $\frac{1}{9}$ is the identity element of Q with respect to $*$.

Since $\frac{1}{27} * \frac{1}{3} = 9\left(\frac{1}{27}\right)\left(\frac{1}{3}\right) = \frac{1}{9} = \text{identity}$, so $\frac{1}{27}$ is the inverse of $\frac{1}{3}$.

2-1.45 Definition: An element a of a group G is said to be *idempotent* if $a^2 = a$.

2-1.46 Theorem: *The only idempotent element in a group is the identity element.*

Proof: Let $a \in G$ be an idempotent element, then

$$a^2 = a$$

$$\Rightarrow a^{-1}a^2 = a^{-1}a$$

$$\Rightarrow a^{-1}aa = e$$

$$\Rightarrow ea = e$$

$$\Rightarrow a = e$$

2-1.47 Theorem: *For any two elements a and b of a group G, the equations $ax = b$ and $ya = b$ have unique solutions.*

Proof: For $a, b \in G, ax = b \Rightarrow a^{-1}(ax) = a^{-1}b$

$\Rightarrow (a^{-1}a)x = a^{-1}b \Rightarrow ex = a^{-1}b \Rightarrow x = a^{-1}b$

So $x = a^{-1}b$ is the solution of $ax = b$.

If x_1 and x_2 are tw osolutions of $ax = b$, then these must satisfy the equation $ax = b$, that is $ax_1 = b$ and $ax_2 = b$.

Hence $ax_1 = b = ax_2 \Rightarrow ax_1 = ax_2 \Rightarrow a^{-1}(ax_1) = a^{-1}(ax_2)$

$\Rightarrow (a^{-1}a)x_1 = (a^{-1}a)x_2 \Rightarrow ex_1 = ex_2 \Rightarrow x_1 = x_2$.

This show sthat the solution of $ax = b$ is unique.

For $a, b \in G, ya = b \Rightarrow (ya)a^{-1} = ba^{-1} \Rightarrow y(aa^{-1}) = ba^{-1}$

$\Rightarrow ye = ba^{-1} \Rightarrow y = ba^{-1}$. So $y = ba^{-1}$ is the solution of $ya = b$. If y_1 and y_2 are tw osolutions of $ya = b$, then these must satisfy the equation $ya = b$, i.e. $y_1a = b$ and $y_2a = b$.

Hence $y_1a = b = y_2a \Rightarrow y_1a = y_2a \Rightarrow (y_1a)a^{-1} = (y_2a)a^{-1}$

$\Rightarrow y_1(aa^{-1}) = y_2(aa^{-1}) \Rightarrow y_1e = y_2e \Rightarrow y_1 = y_2$.

This show sthat the solution of $ya = b$ is unique.

2-1.48 Theorem:

If G is a group, then $(a^{-1})^{-1} = a \quad \forall a \in G$.

Proof: Since G is a group, so

$a \in G$

$\Rightarrow a^{-1} \in G$ $\quad \because G$ is group

$\Rightarrow (a^{-1})^{-1} \in G$ $\quad \because G$ is group

If e is the identity element of G, then

$(a^{-1})^{-1}a^{-1} = e$ (inverse law)

$\Rightarrow [(a^{-1})^{-1}a^{-1}]a = ea$

$\Rightarrow (a^{-1})^{-1}(a^{-1}a) = a$ (associative and identity laws)

$\Rightarrow (a^{-1})^{-1}e = a$ (inverse law)

$\Rightarrow (a^{-1})^{-1} = a$ (identity law)

2-1.49 Theorem:

If G is a group, then $(ab)^{-1} = b^{-1}a^{-1} \; \forall a, b \in G$.

PU, 2012 (B.A./B.Sc.)

Proof: Since G is a group, so

$$a, b \in G$$
$$\Rightarrow ab \in G$$
$$\Rightarrow (ab)^{-1} \in G$$

If e is the identity element of G, then

$$(ab)^{-1}ab = e$$
$$\Rightarrow (ab)^{-1}ab(b^{-1}a^{-1}) = e(b^{-1}a^{-1})$$
$$\Rightarrow (ab)^{-1}a(bb^{-1})a^{-1} = (b^{-1}a^{-1})$$
$$\Rightarrow (ab)^{-1}aea^{-1} = b^{-1}a^{-1}$$
$$\Rightarrow (ab)^{-1}aa^{-1} = b^{-1}a^{-1}$$
$$\Rightarrow (ab)^{-1}e = b^{-1}a^{-1}$$
$$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$$

Similarly, we can show that

$$(ab)^{-1} = b^{-1}a^{-1}$$

In general, $(a_1a_2...a_{k-1}a_k)^{-1} = a_k^{-1}a_{k-1}^{-1}...a_2^{-1}a_1^{-1}$

2-1.50 Theorem: *For any element a of a group G,*

1. $a^n = aa...a$ (n factors)
2. $(a^{-1})^n = a^{-n}$

Proof: We shall prove these assertions by induction.

1. For $n = 2, a^2 = aa$, so C - I is satisfied.

   Let $a^k = aa...a(k \text{ factors})$

   $\Rightarrow aa^k = aaa...a(k+1 \text{ factors})$

   $\Rightarrow a^{k+1} = aaa...a(k+1 \text{ factors}) \Rightarrow$ C - II is satisfied.

   Hence $a^n = aa...a(n \text{ factors})$.

2. For $n = 1, (a^{-1})^1 = a^{-1}$, so C - I is satisfied.

   Let $(a^{-1})^k = a^{-k}$, then $(a^{-1})^k a^{-1} = a^{-k}a^{-1}$

   $\Rightarrow (a^{-1})^{k+1}a^{-1} = a^{-(k+1)} \Rightarrow$ C - II is satisfied.

   Hence $(a^{-1})^n = a^{-n}$.

2-1.51 Example: *Show that a group G is abelian if and only if*

$$(ab)^2 = a^2b^2 \quad \forall a, b \in G$$

PU, 2013 (BS Math)

Solution: Let G be an abelian group, then

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b \qquad \text{(applying associative law)}$$

$$(ab)^2 = a(ab)b \quad \text{(since } G \text{ is an abelian group)}$$
$$= (aa)(bb) \quad \text{(applying associative law)}$$
$$= a^2b^2$$

Conversely, suppose that $(ab)^2 = a^2b^2 \ \forall a, b \in G$, then

$$(ab)^2 = a^2b^2$$
$$\Rightarrow (ab)(ab) = (aa)(bb)$$
$$\Rightarrow a(ba)b = a(ab)b \quad \text{(applying associative law)}$$
$$\Rightarrow a^{-1}a(ba)bb^{-1} = a^{-1}a(ab)bb^{-1}$$
$$\Rightarrow e(ba)e = e(ab)e$$
$$\Rightarrow ba = ab \quad \forall a, b \in G$$

This shows that G is an abelian group.

2-1.52 Example:

If G is an abelian group then show $(ab)^n = a^nb^n$ for all $a, b \in G, n \in Z$.

PU, 1999 (B.A./B.Sc.)

Solution: We shall prove it by mathematical induction.

Case-I: When n is a positive integer.

For $n = 1, (ab)^1 = a^1b^1 = ab$, which is true.

Suppose that the result is true for $n = k$. that is

$$(ab)^k = a^kb^k$$
$$\Rightarrow (ab)^k(ab) = a^kb^k(ab)$$
$$\Rightarrow (ab)^{k+1} = a^k(b^ka)b \quad \text{(using associative law)}$$
$$\Rightarrow (ab)^{k+1} = a^k(ab^k)b \quad (\because G \text{ is abelian } \therefore b^ka = ab^k)$$
$$= (a^ka)(b^kb) \quad \text{(using associative law)}$$
$$= a^{k+1}b^{k+1}$$

Thus, the result is true for $n = k+1$. This shows that $(ab)^n = a^nb^n$ for all positive integral values of n.

Case-II: When n is a negative integer.

Let $n = -m$, where m is a positive integer.

$$(ab)^n = (ab)^{-m} = \left[(ab)^m\right]^{-1}$$
$$= \left[a^mb^m\right]^{-1} \quad \text{(by case-I)}$$
$$= \left[b^ma^m\right]^{-1} \quad (\because G \text{ is abelian } \therefore a^mb^m = b^ma^m)$$
$$= (a^m)^{-1}(b^m)^{-1}$$
$$= a^{-m}b^{-m} = a^nb^n$$

This shows that $(ab)^n = a^nb^n$ for all negative integers n.

Case-III: When $n = 0$, then

$$(ab)^n = (ab)^0 = e = ee = a^0 b^0 = a^n b^n$$

Hence $(ab)^n = a^n b^n$ for all $a, b \in G, n \in Z$.

2-1.53 Example: *Show that if a group G is such that $a \cdot a = e$, for all $a \in G$, where e an identity element of G, then G is an abelian group.*

Solution: Let $a, b \in G$, then by the given definition of G $a \cdot a = e$ and $b \cdot b = e$. Now

$$a \cdot a = e$$
$$\Rightarrow a^{-1} \cdot (a \cdot a) = a^{-1} \cdot e$$
$$\Rightarrow (a^{-1} \cdot a) \cdot a = a^{-1}$$
$$\Rightarrow e \cdot a = a^{-1}$$
$$\Rightarrow a = a^{-1}$$

Similarly, we can show that $b = b^{-1}$. Since G is a group, so

$$a, b \in G$$
$$\Rightarrow a \cdot b \in G$$
$$\Rightarrow (a \cdot b) \cdot (a \cdot b) = e$$
$$\Rightarrow a \cdot b = (a \cdot b)^{-1}$$

Now $a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$

This shows that G is an abelian group.

2-1.54 Example: *If G is a group such that $(ab)^n = a^n b^n$ for three consecutive natural numbers n and all $a, b \in G$, then show that G is an abelian group.*

PU, 2013; 2003; 2002; 2001 (B.A./B.Sc.)

Solution: Let $k, k+1, k+2$ be the three consecutive natural numbers satisfying the equation $(ab)^n = a^n b^n$, then

$$(ab)^k = a^k b^k \quad \ldots(1)$$
$$(ab)^{k+1} = a^{k+1} b^{k+1} \quad \ldots(2)$$
$$(ab)^{k+2} = a^{k+2} b^{k+2} \quad \ldots(3)$$
$$(3) \Rightarrow (ab)^{k+1}(ab) = a^{k+1} ab^{k+1} b$$
$$\Rightarrow (a^{k+1} b^{k+1})(ab) = a^{k+1} ab^{k+1} b \quad \text{(by (2))}$$
$$\Rightarrow a^{k+1}(b^{k+1} a)b = a^{k+1}(ab^{k+1})b \quad \text{(by associative law)}$$
$$\Rightarrow a^{-1}[a^{k+1}(b^{k+1} a)b]b^{-1} = a^{-1}[a^{k+1}(ab^{k+1})b]b^{-1}$$
$$\Rightarrow a^k (b^{k+1} a) = a^k (ab^{k+1})$$
$$\Rightarrow a^k (b^k ba) = a^{k+1} b^{k+1})$$

$$\Rightarrow (a^k b^k)(ba) = (ab)^{k+1} \quad \text{(by (2))}$$
$$\Rightarrow (ab)^k (ba) = (ab)^{k+1} \quad \text{(by (1))}$$
$$\Rightarrow (ab)^k (ba) = (ab)^k (ab)$$
$$\Rightarrow ba = ab \quad \text{(by left cancellation law)}$$

This shows that G is an abelian group.

2-1.55 Example: *If each element of a group G is its own inverse, then show that G is an abelian group.*

Solution: Let $a, b \in G$, then by the given definition of G $a = a^{-1}$ and $b = b^{-1}$. Since G is a group, so

$$a, b \in G$$
$$\Rightarrow ab \in G$$
$$\Rightarrow (ab) = (a.b)^{-1}$$
$$\text{Now } ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

This shows that G is an abelian group.

2-1.56 Example: *If a group G has three elements, then show that G is an abelian group.*

Solution: Let $G = \{e, a, b\}$, where $e \neq a \neq b \neq e$. The multiplication table for G is

$\cdot$	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

This table shows that $a^2 \in G$. So the following three possibilities arise:

(i) either $a^2 = e$ or (ii) $a^2 = a$ or (iii) $a^2 = b$

(i) If $a^2 = e$

The product table also shows that $ab \in G$, so there are further three cases either $ab = e$ or $ab = a$ or $ab = b$. Now

$$ab = e$$
$$\Rightarrow a(ab) = ae$$
$$\Rightarrow a^2 b = e$$
$$\Rightarrow eb = a \qquad \because a^2 = e$$
$$\Rightarrow b = a$$

This is not possible.

Now $ab = a \Rightarrow b = e$ which is also not possible.

Finally $ab = b \Rightarrow a = e$ which is again not possible.

The failure of these three possibilities shows that $a^2 \neq e$.

(ii) If $a^2 = a$, then $a = e$.

Hence $a^2 \neq a$.

Thus the case (iii) is valid, that is $a^2 = b$.

This shows that the group G consists of e, a, a^2. These elements clearly obey the commutative law with respect to multiplication showing that G is an abelian group.

2-2 Order of an Element of a Group

In this section we shall discuss further concepts in details and we shall also discuss the groups in light of these new defined concepts. This section will be very helpful in studying the next sections. Just like the previous section, examples are solved in details in this section.

2-2.1 Definition: The number of elements in a group G is called the *order of group* G and is denoted by $o(G)$ or $|G|$. If the group G consists of finite number of elements then it is said to be a *finite group* otherwise it is said to be an *infinite group*.

2-2.2 Definition: If G is a group and $a \in G$, the *order* or *period* of a is the least positive integer n such that $a^n = e$.

The order of a is denoted by $o(a)$ or $|a|$.

In the group $G = \{-1,1,-i,i\}$, the order of ± 1 is 2 while the order of $\pm i$ is 4.

For any element $a \in G$, we always take $a^0 = e$. If $n = 0$ is the only integer for which $a^n = e$ then a is said to be of *infinite order*.

2-2.3 Theorem: *If n is the order of an element a of a group G, then for any integer m, $a^m = e$ if and only if $m = qn$, where q is an integer.*

OR: *If n is the order of an element a of a group G, then $a^m = e$ if and only if n divides m.*

Proof: Let $a^m = e$ for some integer m, then n, being the order of a, will be lesser or equal to m. By the division algorithm, there are integers q and r such that

$$m = nq + r, 0 \leq r < n \qquad \ldots(1)$$

$$\Rightarrow a^m = a^{nq+r}$$

$$\Rightarrow e = a^{nq}a^r = (a^n)^q a^r = ea^r = a^r$$

$$\Rightarrow a^r = e$$

Since n is the order of a and $r < n$, so $a^r = e$ is only possible if $r = 0$.
Hence (1) takes the form $m = nq$.
Conversely, suppose that $m = qn$, then

$$a^m = a^{nq} = (a^n)^q = e^q = e$$

2-2.4 Example: *Show that in a group, the order of an element is same as that of its inverse.*

Solution: Let G be a group and a be its arbitrary element. Let m and n be orders of a and a^{-1} respectively, then

$$a^m = e \quad \ldots(1)$$

and

$$(a^{-1})^n = e \quad \ldots(2)$$

$$\Rightarrow a^{-n} = e$$

$$\Rightarrow a^n \cdot a^{-n} = a^n \cdot e$$

$$\Rightarrow e = a^n \quad \ldots(3)$$

Since m is the order of a, so (3) shows that m divides n.
Similarly

$$(1) \Rightarrow a^{-m} \cdot a^m = a^{-m} \cdot e$$

$$\Rightarrow e = a^{-m}$$

$$\Rightarrow e = (a^{-1})^m \quad \ldots(4)$$

Since n is the order of a^{-1}, so (4) shows that n divides m.
Hence $m = n$
i.e. $o(a) = o(a^{-1})$

2-2.5 Example:
Show that in a group G, $o(ab) = o(ba)$ $\forall a, b \in G$.

Solution: Let m and n be the orders of ab and ba respectively, then

$$(ab)^m = e \quad \ldots(1)$$

and

$$(ba)^n = e \quad \ldots(2)$$

$$\Rightarrow ba.ba.....ba = e \qquad (n \text{ factors})$$

$$\Rightarrow ab.ab.....a = b^{-1}e$$

$$\Rightarrow ab.ab.....a = b^{-1}$$

$$\Rightarrow ab.ab.....ab = b^{-1}b$$

$$\Rightarrow ab.ab.....ab = e$$

$$\Rightarrow (ab)^n = e \quad \ldots(3)$$

Since m is the order of ab, so (3) shows that m divides n.
Similarly, from (1), we have

$$ab.ab.....ab = e \qquad (m \text{ factors})$$

$$\Rightarrow baba.....b = a^{-1}e$$
$$\Rightarrow baba.....b = a^{-1}$$
$$\Rightarrow baba.....ba = a^{-1}a$$
$$\Rightarrow baba.....ba = e$$
$$\Rightarrow (ba)^m = e \qquad ...(4)$$

Since n is the order of ba, so (4) shows that n divides m.
Hence $m = n$, i.e., $o(ab) = o(ba)$.

2-2.6 Example: *Show that in a group G,* $o(a) = o(bab^{-1})$ $\forall a, b \in G$.

Solution: Let m and n be the orders of a and (bab^{-1}) respectively, then

$$a^m = e \qquad ...(1)$$
$$\text{and } (bab^{-1})^n = e \qquad ...(2)$$
$$\Rightarrow (bab^{-1}) \cdot (bab^{-1}) \cdot ..... \cdot (bab^{-1}) = e \qquad (n \text{ factors})$$
$$\Rightarrow b \cdot a^n \cdot b^{-1} = e$$
$$\Rightarrow b^{-1} \cdot (b \cdot a^n \cdot b^{-1}) \cdot b = b^{-1} \cdot e \cdot b$$
$$\Rightarrow (b^{-1} \cdot b) \cdot a^n \cdot (b^{-1} \cdot b) = b^{-1} \cdot b$$
$$\Rightarrow e \cdot a^n \cdot e = e$$
$$\Rightarrow a^n = e \qquad ...(3)$$

Since m is the order of a, so (3) shows that m divides n.

Similarly (1)

$$\Rightarrow a^m = e$$
$$\Rightarrow e \cdot a^m \cdot e = e$$
$$\Rightarrow (b^{-1} \cdot b) \cdot a^m \cdot (b^{-1} \cdot b) = e$$
$$\Rightarrow b^{-1} \cdot (b \cdot a^m \cdot b^{-1}) \cdot b = e$$
$$\Rightarrow b \cdot b^{-1} \cdot (b \cdot a^m \cdot b^{-1}) \cdot b \cdot b^{-1} = b \cdot e \cdot b^{-1}$$
$$\Rightarrow e \cdot (b \cdot a^m \cdot b^{-1}) \cdot e = b \cdot b^{-1}$$
$$\Rightarrow (b \cdot a^m \cdot b^{-1}) = e$$
$$\Rightarrow (bab^{-1}) \cdot (bab^{-1}) \cdot ..... \cdot (bab^{-1}) = e \qquad (m \text{ factors})$$
$$\Rightarrow (bab^{-1})^m = e \qquad ...(4)$$

Since n is the order of $b \cdot a \cdot b^{-1}$, so (4) shows that n divides m.
Hence $m = n$, i.e., $o(a) = o(bab^{-1})$.

2-2.7 Example: *Show that in a group G,* $o(a) = o(b^{-1}ab)$ $\forall a, b \in G$.

Solution: Let m and n be the orders of a and $(b^{-1}ab)$ respectively, then

$$a^m = e \quad \ldots(1)$$

$$\text{and } (b^{-1}ab)^n = e \quad \ldots(2)$$

$$\Rightarrow (b^{-1}ab)\cdot(b^{-1}ab)\cdot\ldots\cdot(b^{-1}ab) = e \quad (n \text{ factors})$$

$$\Rightarrow b^{-1}\cdot a^n \cdot b = e$$

$$\Rightarrow b\cdot(b^{-1}\cdot a^n \cdot b)\cdot b^{-1} = b\cdot e\cdot b^{-1}$$

$$\Rightarrow (b\cdot b^{-1})\cdot a^n \cdot (b\cdot b^{-1}) = b\cdot b^{-1}$$

$$\Rightarrow e\cdot a^n \cdot e = e$$

$$\Rightarrow a^n = e \quad \ldots(3)$$

Since m is the order of a, so (3) shows that m divides n.

Similarly $(1) \Rightarrow a^m = e$

$$\Rightarrow e.a^m.e = e$$

$$\Rightarrow (b\cdot b^{-1})\cdot a^m \cdot (b\cdot b^{-1}) = e$$

$$\Rightarrow b\cdot(b^{-1}\cdot a^m \cdot b)\cdot b^{-1} = e$$

$$\Rightarrow b^{-1}\cdot b\cdot(b\cdot a^m \cdot b)\cdot b^{-1}\cdot b = b^{-1}\cdot e\cdot b$$

$$\Rightarrow e\cdot(b^{-1}\cdot a^m \cdot b)\cdot e = b^{-1}\cdot b$$

$$\Rightarrow (b^{-1}\cdot a^m \cdot b) = e$$

$$\Rightarrow (b^{-1}ab)\cdot(b^{-1}ab)\cdot\ldots\cdot(b^{-1}ab) = e \quad (m \text{ factors})$$

$$\Rightarrow (b^{-1}ab)^m = e \quad \ldots(4)$$

Since n is the order of $b^{-1}ab$, so (4) shows that n divides m.

Hence $m = n$, i.e. $o(a) = o(b^{-1}ab)$.

2-2.8 Example: *If every non-identity element of a group G is of order two then show that G is abelian.*

Solution: Let a and b be arbitrary elements of the group G, then

$$a^2 = e \text{ and } b^2 = e$$

$$\Rightarrow a = a^{-1} \text{ and } b = b^{-1}$$

$$\text{Now } a, b \in G \Rightarrow ab \in G$$

$$\Rightarrow (ab)^2 = e$$

$$\Rightarrow ab = (ab)^{-1}$$

$$\text{Since } (ab)^{-1} = b^{-1}a^{-1} \quad \ldots(1)$$

so using above values in (1), we have

$$ab = ba \quad \ldots(2)$$

Since a, b were arbitrary elements of G, so (2) shows that

$$ab = ba \ \forall a, b \in G$$

This shows that G is an abelian group.

2-2.9 Example: *If a group G has only one element a of order two then show that $ax = xa$ for all $x \in G$.*

Solution: Since G, is a group and $a \in G$, so $x^{-1}ax \in G \forall x \in G$.

Next consider

$$\begin{aligned}(x^{-1}ax)^2 &= (x^{-1}ax)(x^{-1}ax)\\ &= (x^{-1}a)xx^{-1}(ax)\\ &= (x^{-1}a)e(ax)\\ &= (x^{-1}a)(ax)\\ &= x^{-1}(aa)x\\ &= x^{-1}a^2x\\ &= x^{-1}ex \quad \because a \text{ is of order 2, so } a^2 = e\\ &= x^{-1}x\\ &= e\end{aligned}$$

This shows that $o(x^{-1}ax) = 2$. But a is the only element of G whose order is 2, so

$$\begin{aligned}&(x^{-1}ax) = a\\ \Rightarrow\ &x(x^{-1}ax) = xa\\ \Rightarrow\ &xx^{-1}(ax) = xa\\ \Rightarrow\ &e(ax) = xa\\ \Rightarrow\ &ax = xa \quad \forall x \in G\end{aligned}$$

2-2.10 Example: *If in a group G, $b = xax^{-1}$. Show that $b^2 = xa^2x^{-1}$ and hence show that the elements a and b are of the same order.*

Solution: Consider

$$\begin{aligned}b^2 &= (xax^{-1})(xax^{-1})\\ &= xa(x^{-1}x)ax^{-1}\\ &= xaeax^{-1}\\ &= xaax^{-1}\\ &= xa^2x^{-1}\end{aligned}$$

Let m and n be the orders of a and b respectively, then

$$a^m = e \qquad \ldots(1)$$

and

$$b^n = e \qquad \ldots(2)$$

$$\Rightarrow xa^n x^{-1} = e \qquad \because b^n = xa^n x^{-1}$$
$$\Rightarrow x^{-1}(xa^n x^{-1})x = x^{-1}ex$$
$$\Rightarrow (x^{-1}x)a^n(x^{-1}x) = x^{-1}x$$
$$\Rightarrow ea^n e = e$$
$$\Rightarrow ea^n e = e$$
$$\Rightarrow a^n = e \qquad \ldots(3)$$

Since m is the order of a, so (3) shows that m divides n.
Similarly, (1)

$$\Rightarrow xa^m x^{-1} = xex^{-1}$$
$$\Rightarrow b^m = xx^{-1} \qquad \because b^m = xa^m x^{-1}$$
$$\Rightarrow b^m = e \qquad \ldots(4)$$

Since n is the order of b, so (4) shows that n divides m.
Hence $m = n$, i.e. $o(a) = o(b)$.

2-2.11 Example:

If in a group G, $xa = ax$, then show that $xa^2 = a^2x$ and $x^2a = ax^2$.

Solution:

$$xa = ax \qquad \ldots.(1)$$
$$\Rightarrow (xa)a = (ax)a$$
$$\Rightarrow x(aa) = a(xa)$$
$$\Rightarrow xa^2 = a(ax) \qquad \because xa = ax$$
$$\Rightarrow xa^2 = (aa)x$$
$$\Rightarrow xa^2 = a^2x$$
$$(1) \Rightarrow x(xa) = x(ax)$$
$$\Rightarrow (xx)a = (xa)x$$
$$\Rightarrow x^2a = (ax)x \qquad \because xa = ax$$
$$\Rightarrow x^2a = a(xx)$$
$$\Rightarrow x^2a = ax^2$$

2-2.12 Example:

Determine the order of $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Solution:

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^3 = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^2\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^4 = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^3\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

This shows that the order of $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$ is 4.

2-2.13 Example:
If G is a finite group such that $xy = yz \Rightarrow x = z$ for $x, y, z \in G$, then show that G is abelian.

Solution: Let $a, b \in G$, then using associative law, we have

$$(ab)a = a(ba)$$
$$\Rightarrow (ab) = (ba) \qquad \text{(using given condition)}$$
$$\Rightarrow ab = ba \quad \forall a, b \in G.$$

This shows that G is an abelian group.

2-2.14 Example: *If in the group G, $a^5 = e, aba^{-1} = b^2$ for $a, b \in G$, then find the order of b.*

Solution: Consider

$$b = ebe = a^5ba^{-5} \qquad \because a^5 = e = a^{-5}$$
$$= a^4(aba^{-1})a^{-4}$$
$$= a^4(b^2)a^{-4} \qquad \because aba^{-1} = b^2$$
$$= a^3(ab^2a^{-1})a^{-3}$$
$$= a^3(b^4)a^{-3} \qquad \because ab^2a^{-1} = b^4$$
$$= a^2(ab^4a^{-1})a^{-2}$$
$$= a^2(b^8)a^{-2} \qquad \because ab^4a^{-1} = b^8$$
$$= a(ab^8a^{-1})a^{-1}$$
$$= a(b^{16})a^{-1} \qquad \because ab^8a^{-1} = b^{16}$$
$$= b^{32} \qquad \because (ab^{16}a^{-1}) = b^{32}$$
$$\Rightarrow b^{31} = e$$
$$\Rightarrow o(b) = 31$$

2-2.15 Example: *Let an element a of a group G be of an odd order, then show that there exists an element b in G such that $b^2 = a$.*

Solution: Since a is of an odd order, so let $2m+1, m \geq 0$, be the order of a. Then $a^{2m+1} = e$

$\because a^{m+1} \in G$, so let $b = a^{m+1}$

$\Rightarrow b^2 = (a^{m+1})^2 = a^{2m+2} = a^{2m+1}a = ea = a$

$\Rightarrow b^2 = a$

2-2.16 Example: *In a group of even order, show that there is at least one element of order two.*

Solution: Let G be a group of even order. Further suppose that

$$G = \{e, a_1, a_2, ..., a_{2n-1}\}$$

This clearly shows that there is an odd number of non-identity elements in G. Let $o(a) \neq 2 \; \forall a \in G, a \neq e$, then the inverse of each non-identity element must be another non-identity element. If we collect the non-identity elements along their inverses then, due to odd in numbers, there must be one non-identity element of G without its inverse. This is impossible, so $o(a) = 2$ for at least one non-identity element a of G.

2-3 Subgroups

Before turning to the study of groups we should like to change our notation slightly. It is cumbersome to keep using the '$\cdot$' for the group operation; henceforth we shall drop it and instead of writing $a.b$ for $a, b \in G$ we shall simply denote this product as ab.

In general we shall not be interested in arbitrary subsets of a group G for they do not reflect the fact that G has an algebraic structure imposed on it. Whatever subsets we do consider will be those endowed with algebraic properties derived from those of G.

In this section we shall study those subsets of groups which themselves will be groups.

2-3.1 Definition: A subset H of a group G is called the *subgroup* of G if H itself is a group under the same binary operation as defined in G.

According to this definition, an arbitrary subset of a group G need not necessarily be a subgroup of G. A subset H of a group G may itself be a group under an operation different from that of in G, in this case H will not be a subgroup G. For instance the set $H = \{\pm 1, \pm i\}$ is a subset of set of complex numbers C and H itself is a group under multiplication. But H is not a subgroup of C, because C is a group under addition.

2-3.2 Definition: Every group G has at least two subgroups namely G itself and the identity group $\{e\}$. These are called the *trivial subgroups* of G. Any other subgroup of G is called a *non-trivial subgroup* of G.

2-3.3 Examples:

1. The set Z of integers under addition is a subgroup of the group Q of rational numbers under addition, Q is a subgroup of the group R of real numbers under addition and R is a subgroup of the group C of complex numbers under addition.
2. The set $\{\pm 1\}$ is a subgroup of $\{\pm 1, \pm i\}$ under complex multiplication.
3. The set R^+ of all positive real numbers under multiplication is a subgroup of the group R' of all non-zero real numbers under multiplication.
4. The set of cube roots of unity is also a subgroup of a group of non-zero complex numbers under multiplication.
5. The set $\{\pm 1\}$ is a subgroup of the group of non-zero rational numbers under ordinary multiplication.

The following theorem gives a necessary and sufficient condition for a subset of a group to be a subgroup.

2-3.4 Theorem: *Let $(G,*)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a,b \in H$, the element $a * b' \in H$, .where b' is the inverse of b.*

Proof: Let H be a subgroup of G. Let $a,b \in H$. Since H is a subgroup of G, so by the definition of subgroup, $(H,*)$ is a group. Since the inverse of each element of a group also belongs to the group, so

$$b \in H$$
$$\Rightarrow b' \in H$$

Since the group is always closed under the binary operation defined on it, so H is also closed under $*$, i.e.

$$a, b' \in H$$
$$\Rightarrow a * b' \in H$$

Hence $$a * b' \in H \qquad \forall a,b \in H$$

Conversely, let $a * b' \in H$ for all $a,b \in H$, where b' is the inverse of b. Then we have to show that H is a subgroup of G. For this we shall show that $(H,*)$ is a group. By the given condition,

$$a, a \in H$$
$$\Rightarrow a * a' \in H \quad \forall a \in H$$
$$\Rightarrow e \in H$$

Since H is a subset of G, so

$$e \in H$$
$$\Rightarrow e \in G$$

This shows that e is an identity element of G. Since H is a subset of G, so e will also the identity element of H.

This shows that the identity element of H is also in H.

Once again, by the given condition

$$e, a \in H$$

$$\Rightarrow e * a' \in H \quad \forall a \in H$$

$$\Rightarrow a' \in H \quad \forall a \in H$$

This shows that the inverse of each element of H is also in H.

Let $a, b \in H$, then $b \in H \Rightarrow b' \in H$, so by the given condition

$$a, b' \in H$$

$$\Rightarrow a * (b')' \in H$$

$$\Rightarrow a * b \in H \quad \forall a, b \in H$$

This shows that H is closed under $*$.

Finally, the associative law holds in H, because it holds in G.

Since all the axioms under $*$ of a group are satisfied in H, so $(H, *)$ is a group. Hence H is a subgroup of G.

2-3.5 Theorem: *Let $(G, \cdot)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a, b \in H$, the element $ab^{-1} \in H$.*

Proof: Let H be a subgroup of G. Let $a, b \in H$. Since H is a subgroup of G, so by the definition of subgroup, $(H, \cdot)$ is a group. Since the inverse of each element of a group also belongs to the group, so

$$b \in H$$

$$\Rightarrow b^{-1} \in H$$

Since the group is always closed under the binary operation defined on it, so H is also closed under '$\cdot$', i.e.

$$a, b^{-1} \in H$$

$$\Rightarrow ab^{-1} \in H$$

Hence $ab^{-1} \in H \; \forall a, b \in H$.

Conversely, let $ab^{-1} \in H$ for all $a, b \in H$, then we have to show that H is a subgroup of G. For this we shall show that $(H, \cdot)$ is a group. By the given condition,

$$a, a \in H$$

$$\Rightarrow aa^{-1} \in H \quad \forall a \in H$$

$$\Rightarrow e \in H$$

Since H is a subset of G, so

$$e \in H$$

$$\Rightarrow e \in G$$

This shows that e is an identity element of G. Since H is a subset of G, so e will also the identity element of H. This shows that the identity element of H is also in H.

Once again, by the given condition

$$e, a \in H$$
$$\Rightarrow ea^{-1} \in H \quad \forall a \in H$$
$$\Rightarrow a^{-1} \in H \quad \forall a \in H$$

This shows that the inverse of each element of H is also in H.
Let $a, b \in H$, then

$$b \in H$$
$$\Rightarrow b^{-1} \in H$$

so by the given condition

$$a, b^{-1} \in H$$
$$\Rightarrow a(b^{-1})^{-1} \in H$$
$$\Rightarrow ab \in H \quad \forall a, b \in H$$

This shows that H is closed under multiplication.
Finally, the associative law holds in H, because it holds in G.
Since all the axioms under multiplication of a group are satisfied in H, so $(H, \cdot)$ is a group. Hence H is a subgroup of G.

2-3.6Theorem: *Let $(G, +)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a, b \in H$, the element $a + (-b) \in H$.*

PU, 2000 (B.A./B.Sc.)

Proof: Let H be a subgroup of G. Let $a, b \in H$. Since H is a subgroup of G, so by the definition of subgroup, $(H, +)$ is a group. Since the inverse of each element of a group also belongs to the group, so

$$b \in H$$
$$\Rightarrow -b \in H$$

Since the group is always closed under the binary operation defined on it, so H is also closed under '+', i.e.

$$a, -b \in H$$
$$\Rightarrow a + (-b) \in H$$

Hence $$a + (-b) \in H \quad \forall a, b \in H$$

Conversely, let $a + (-b) \in H$ for all $a, b \in H$, then we have to show that H is a subgroup of G. For this we shall show that $(H, +)$ is a group. By the given condition,

$$a, a \in H$$
$$\Rightarrow a + (-a) \in H \quad \forall a \in H$$
$$\Rightarrow e \in H$$

Since H is a subset of G, so

$$e \in H$$
$$\Rightarrow e \in G$$

This shows that e is an identity element of G. Since H is a subset of G, so e will also the identity element of H. This shows that the identity element of H is also in H.

Once again, by the given condition

$$e, a \in H$$
$$\Rightarrow e + (-a) \in H \qquad \forall a \in H$$
$$\Rightarrow -a \in H \qquad \forall a \in H$$

This shows that the inverse of each element of H is also in H.

Let $a, b \in H$, then $b \in H \Rightarrow -b \in H$, so by the given condition

$$a, -b \in H$$
$$\Rightarrow a + [-(-b)] \in H$$
$$\Rightarrow a + b \in H \quad \forall a, b \in H$$

This shows that H is closed under addition.

Finally, the associative law holds in H, because it holds in G.

Since all the axioms under addition of a group are satisfied in H, so $(H,+)$ is a group. Hence H is a subgroup of G.

2-3.7 Theorem: *Let $(G,*)$ be a group. A nonempty subset H of G is a subgroup of G if and only if*

1. $a, b \in H \Rightarrow a * b \in H$,
2. $a \in H \Rightarrow a' \in H$, where a' is a the inverse of a.

Proof: Let H be a subgroup of G, then $(H,*)$ is a group.

1. Let $a, b \in H$, then $a * b \in H$, since $(H,*)$ is a group.
2. Let $a \in H$, then $a' \in H$, since $(H,*)$ is a group.

Conversely, let

1. $a, b \in H \Rightarrow a * b \in H$,
2. $a \in H \Rightarrow a' \in H$.

Then we have to show that H is a subgroup, for this it is enough to show that $(H,*)$ is a group.

G_1): (1) $\Rightarrow a * b \in H \; \forall a, b \in H$.

G_2): The associative law holds in H, because it holds in G and H is a subset of G.

G_3): Let $a \in H$, then by (2) $a' \in H$.

Now by (1) $a, a' \in H \Rightarrow a * a' \in H \Rightarrow e \in H$.

G_4): (2) $\Rightarrow a' \in H \; \forall a \in H$.

This shows that $(H,*)$ is a group. Hence H is a subgroup of G.

2-3.8 Theorem: *Let $(G,\cdot)$ be a group. A nonempty subset H of G is a subgroup of G if and only if*

1. $a, b \in H \Rightarrow ab \in H$,

2. $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let H be a subgroup of G, then $(H,\cdot)$ is a group.

1. Let $a,b \in H$, then $ab \in H$, since $(H,\cdot)$ is a group.
2. Let $a \in H$, then $a^{-1} \in H$, since $(H,\cdot)$ is a group.

Conversely, let

1. $a,b \in H \Rightarrow ab \in H$,
2. $a \in H \Rightarrow a^{-1} \in H$.

Then we have to show that H is a subgroup, for this it is enough to show that $(H,\cdot)$ is a group.

G_1): (1) $\Rightarrow ab \in H \ \forall a,b \in H$

G_2): The associative law holds in H, because it holds in G and H is a subset of G.

G_3): Let $a \in H$, then by (2) $a^{-1} \in H$.

Now by (1) $a,a^{-1} \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

G_4): (2) $\Rightarrow a^{-1} \in H \ \forall a \in H$.

This shows that $(H,\cdot)$ is a group. Hence H is a subgroup of G.

2-3.9 Theorem: *Let $(G,+)$ be a group. A nonempty subset H of G is a subgroup of G if and only if*

1. $a,b \in H \Rightarrow a+b \in H$,
2. $a \in H \Rightarrow -a \in H$.

Proof: Let H be a subgroup of G, then $(H,+)$ is a group.

1. Let $a,b \in H$, then $a+b \in H$, since $(H,+)$ is a group.
2. Let $a \in H$, then $-a \in H$, since $(H,+)$ is a group.

Conversely, let

1. $a,b \in H \Rightarrow a+b \in H$,
2. $a \in H \Rightarrow -a \in H$.

Then we have to show that H is a subgroup, for this it is enough to show that $(H,+)$ is a group.

G_1): (1) $\Rightarrow a+b \in H \qquad \forall a,b \in H$

G_2): The associative law holds in H, because it holds in G and H is a subset of G.

G_3): Let $a \in H$, then by (2) $-a \in H$.

Now by (1) $a,-a \in H$

$\Rightarrow a+(-a) \in H$

$\Rightarrow e \in H$

G_4): (2) $\Rightarrow -a \in H \qquad \forall a \in H$

This shows that $(H,+)$ is a group. Hence H is a subgroup of G.

2-3.10 Theorem: *Let $(G,\cdot)$ be a group and H be a nonempty finite subset of G such that H is closed under multiplication, then H is a subgroup of G.*

Proof: In order to prove that H is a subgroup of G, we to have show that $(H,\cdot)$ is a group.

G_1): It is given that H is closed under multiplication, so $ab \in H \; \forall a,b \in H$.

G_2): The associative law holds in H, because it holds in G and H is a subset of G.

G_3): Let $a \in H$, then $a^2 = aa \in H, a^3 = a^2 a \in H, \ldots, a^m \in H, \ldots$ since H is closed under multiplication. Thus the infinite collection of elements $a, a^2, a^3, \ldots, a^m, \ldots$ must all belong to H, which is a finite subset of G. Thus there must be repetitions in this collection of elements; that is, for some integers r, s with $r > s > 0, a^r = a^s$.

Since $r - s > 0$, so $a^{r-s} \in H$. But $a^r = a^s \Rightarrow a^{r-s} = e$. Hence $e \in H$.

G_4): Since $r - s - 1 \geq 0$, so $a^{r-s-1} \in H$. Now $aa^{r-s-1} = a^{r-s} = e$, shows that $a^{-1} = a^{r-s-1}$. Thus $a^{-1} \in H$ for all $a \in H$.

This shows that $(H,\cdot)$ is a group. Hence H is a subgroup of G.

2-3.11 Theorem: *Let $(G,+)$ be a group and H be a nonempty finite subset of G such that H is closed under addition, then H is a subgroup of G.*

Proof: In order to prove that H is a subgroup of G, we have to show that $(H,+)$ is a group.

G_1): It is given that H is closed under addition, so $a + b \in H \; \forall a,b \in H$.

G_2): The associative law holds in H, because it holds in G and H is a subset of G.

G_3): Let $a \in H$, then

$$2a = a + a \in H, 3a = 2a + a \in H, \ldots, ma \in H, \ldots$$

Since H is closed under addition. Thus the infinite collection of elements $a, 2a, 3a, \ldots, ma, \ldots$ must all belong to H, which is a finite subset of G. Thus there must be repetitions in this collection of elements; that is, for some integers r, s with $r > s > 0, ra = sa$.

Since $r - s > 0$, so $(r - s)a \in H$.

But $ra = sa \Rightarrow (r - s)a = e$. Hence $e \in H$.

G_4): Since $r - s - 1 \geq 0$, so $(r - s - 1)a \in H$.

Now $a + (r - s - 1)a = (r - s)a = e$, shows that $-a = (r - s - 1)a$. Thus $-a \in H$ for all $a \in H$.

This shows that $(H,+)$ is a group. Hence H is a subgroup of G.

2-3.12 Theorem: *The intersection of any collection of subgroups of a group $(G,*)$ is a subgroup of G.*

Proof: Let G be a group and $\{H_\alpha : \alpha \in I\}$ be a collection of subgroups of G, then we have to show that $\bigcap_{\alpha\in I} H_\alpha$ is also a subgroup of G. For this let

$$a,b \in \bigcap_{\alpha\in I} H_\alpha$$
$$\Rightarrow a,b \in H_\alpha \quad \forall \alpha \in I$$
$$\Rightarrow a * b' \in H_\alpha \quad \forall \alpha \in I \quad \because \text{each } H_\alpha \text{ is a subgroup}$$
$$\Rightarrow a * b' \in \bigcap_{\alpha\in I} H_\alpha$$

This shows that $\bigcap_{\alpha\in I} H_\alpha$ is a subgroup of G.

2-3.13 Theorem: *The intersection of any collection of subgroups of a group $(G,\cdot)$ is a subgroup of G.*

Proof: Let G be a group and $\{H_\alpha : \alpha \in I\}$ be a collection of subgroups of G, then we have to show that $\bigcap_{\alpha\in I} H_\alpha$ is also a subgroup of G. For this let

$$a,b \in \bigcap_{\alpha\in I} H_\alpha$$
$$\Rightarrow a,b \in H_\alpha \quad \forall \alpha \in I$$
$$\Rightarrow ab^{-1} \in H_\alpha \quad \forall \alpha \in I \quad \because \text{each } H_\alpha \text{ is a subgroup}$$
$$\Rightarrow ab^{-1} \in \bigcap_{\alpha\in I} H_\alpha$$

This shows that $\bigcap_{\alpha\in I} H_\alpha$ is a subgroup of G.

2-3.14 Theorem: *The intersection of any collection of subgroups of a group $(G,+)$ is a subgroup of G.*

Proof: Let G be a group and $\{H_\alpha : \alpha \in I\}$ be a collection of subgroups of G, then we have to show that $\bigcap_{\alpha\in I} H_\alpha$ is also a subgroup of G. For this let

$$a,b \in \bigcap_{\alpha\in I} H_\alpha$$
$$\Rightarrow a,b \in H_\alpha \quad \forall \alpha \in I$$
$$\Rightarrow a+(-b) \in H_\alpha \quad \forall \alpha \in I \quad \because \text{each } H_\alpha \text{ is a subgroup}$$
$$\Rightarrow a+(-b) \in \bigcap_{\alpha\in I} H_\alpha$$

This shows that $\bigcap_{\alpha\in I} H_\alpha$ is a subgroup of G.

2-3.15 Theorem: *The union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.*

PU, S2014 (M.Sc. Math); PU, 2013 (BS Math); PU, 2001 (B.A./B.Sc.)

Proof: Let H and K be the subgroups of G. Let

$$H \subset K \qquad \ldots(1)$$

then we have to show that $H \cup K$ is a subgroup of G. Now

$$(1) \Rightarrow H \cup K = K \qquad \ldots(2)$$

Since K is a subgroup of G, so (2) shows that $H \cup K$ is a subgroup of G.
On the other hand, if

$$K \subset H \quad \ldots(3)$$

then

$$H \cup K = H \quad \ldots(4)$$

Since H is a subgroup of G, so (4) shows that $H \cup K$ is a subgroup of G.
Conversely, let $H \cup K$ be a subgroup of G, then we have to show that either $H \subset K$ or $K \subset H$. For this suppose on contrary that neither $H \subset K$ nor $K \subset H$. Then there exist elements a, b such that

$$a \in H \text{ and } a \notin K, \quad b \in K \text{ and } b \notin H$$

Now $\quad a \in H \Rightarrow a \in H \cup K$

And $\quad b \in K \Rightarrow b \in H \cup K$

Since $H \cup K$ is a subgroup, so

$$a, b \in H \cup K$$
$$\Rightarrow ab \in H \cup K$$
$$\Rightarrow ab \in H \text{ or } ab \in K$$

If $ab \in H$, then

$$a^{-1}(ab) \in H \qquad \because a \in H \Rightarrow a^{-1} \in H$$
$$\Rightarrow (a^{-1}a)b \in H$$
$$\Rightarrow eb \in H$$
$$\Rightarrow b \in H$$

which is a contradiction, because $b \notin H$.
If $ab \in K$, then

$$(ab)b^{-1} \in K \quad \because b \in K \Rightarrow b^{-1} \in K$$
$$\Rightarrow a(bb^{-1}) \in K$$
$$\Rightarrow ae \in K$$
$$\Rightarrow a \in K$$

which is a contradiction, because $a \notin K$.
The contradiction in both cases shows that our assumption that neither $H \subset K$ nor $K \subset H$ is wrong. Hence, either $H \subset K$ or $K \subset H$.
This completes the proof.

2-3.16 Theorem: *Let G be an abelian group and H the set of all elements of finite order in G, then H is a subgroup of G.*

Proof: Let $a, b \in H$, then by the definition of H there exist integers m and n such that

$$a^m = e \quad \ldots(1)$$

and

$$b^n = e \quad \ldots(2)$$

Since the order of an element is same as that of its inverse, so from (2), we have

$$(b^{-1})^n = e \quad \ldots(3)$$

Since G is abelian group, so

$$\begin{aligned}(ab^{-1})^{mn} &= a^{mn}(b^{-1})^{mn}\\ &= (a^m)^n[(b^{-1})^n]^m\\ &= (e)^n(e)^m \qquad \text{(by (1) and (3))}\\ &= (e)(e)\\ &= e\end{aligned}$$

This shows that ab^{-1} is of finite order of mn. Hence $ab^{-1} \in H$. Since

$$a, b \in H$$

$$\Rightarrow ab^{-1} \in H$$

so H is a subgroup of G.

2-3.17 Theorem: *Let G be a group and H a subgroup of G then for any $a \in G$, the set $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a subgroup of G.*

PU, 2003 (B.A./B.Sc.)

Proof: Let $x, y \in aHa^{-1}$, then there exist $h_1, h_2 \in H$ such that $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$. Next consider

$$\begin{aligned}xy^{-1} &= (ah_1a^{-1})(ah_2a^{-1})^{-1}\\ &= (ah_1a^{-1})(ah_2^{-1}a^{-1})\\ &= ah_1(a^{-1}a)h_2^{-1}a^{-1}\\ &= ah_1eh_2^{-1}a^{-1}\\ &= ah_1h_2^{-1}a^{-1}\\ &= ah_3a^{-1}, \qquad h_1h_2^{-1} = h_3\end{aligned}$$

Since H is a subgroup of G, so

$$\begin{aligned}&h_1, h_2 \in H\\ &\Rightarrow h_1h_2^{-1} \in H\\ &\Rightarrow h_3 \in H\\ &\Rightarrow ah_3a^{-1} \in aHa^{-1}\\ &\Rightarrow xy^{-1} \in aHa^{-1}\end{aligned}$$

Since $x, y \in aHa^{-1}$

$\Rightarrow xy^{-1} \in aHa^{-1}$, so aHa^{-1} is a subgroup

This completes the proof.

2-3.18 Theorem: *Let G be a group and H a subgroup of G, then the set*

$$a^{-1}Ha = \{a^{-1}ha : h \in H\}$$

is a subgroup of G.

Proof: Let $x, y \in a^{-1}Ha$, then there exist $h_1, h_2 \in H$ such that $x = a^{-1}h_1a$ and $y = a^{-1}h_2a$. Next consider

$$\begin{aligned} xy^{-1} &= (a^{-1}h_1a)(a^{-1}h_2a)^{-1} \\ &= (a^{-1}h_1a)(a^{-1}h_2^{-1}a) \\ &= a^{-1}h_1(aa^{-1})h_2^{-1}a \\ &= a^{-1}h_1eh_2^{-1}a \\ &= a^{-1}h_1h_2^{-1}a \\ &= a^{-1}h_3a, \qquad h_1h_2^{-1} = h_3 \end{aligned}$$

Since H is a subgroup of G, so

$$\begin{aligned} & h_1, h_2 \in H \\ \Rightarrow\ & h_1h_2^{-1} \in H \\ \Rightarrow\ & h_3 \in H \\ \Rightarrow\ & a^{-1}h_3a \in a^{-1}Ha \\ \Rightarrow\ & xy^{-1} \in a^{-1}Ha \end{aligned}$$

Since $x, y \in a^{-1}Ha \Rightarrow xy^{-1} \in a^{-1}Ha$, so $a^{-1}Ha$ is a subgroup.
This completes the proof.

2-3.19 Theorem: *Let $(G, *)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $a' = a$, then H is a subgroup of G.*

Proof: By the definition of H,

$$H = \{a \in G : a' = a\}$$

Let $a, b \in H$ then $a' = a, b' = b$. Next consider

$$\begin{aligned} (a * b')' &= b * a' \\ &= b * a \quad \because a' = a \\ &= a * b \quad \because G \text{ is abelian} \\ &= a * b' \quad \because b' = b \\ \Rightarrow\ & a * b' \in H \end{aligned}$$

Since $a, b \in H \Rightarrow a * b' \in H$, so H is a subgroup of G.

2-3.20 Theorem: *Let $(G, \cdot)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $a^{-1} = a$, then H is a subgroup of G.*

Proof: By the definition of H,

$$H = \{a \in G : a^{-1} = a\}$$

Let $a, b \in H$ then $a^{-1} = a, b^{-1} = b$.

Next consider

$$(ab^{-1})^{-1} = ba^{-1}$$
$$= ba \qquad \because a^{-1} = a$$
$$= ab \qquad \because G \text{ is abelian}$$
$$= ab^{-1} \qquad \because b' = b$$
$$\Rightarrow ab^{-1} \in H$$

Since $a, b \in H \Rightarrow ab^{-1} \in H$, so H is a subgroup of G.

2-3.21 Theorem: *Let $(G,+)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $-a = a$, then H is a subgroup of G.*

Proof: By the definition of H,

$$H = \{a \in G : -a = a\}$$

Let $a, b \in H$ then $-a = a, -b = b$.

Next consider

$$-[a + (-b)] = -a + b$$
$$= a + b \qquad \because -a = a$$
$$= a + (-b) \qquad \because -b = b$$
$$\Rightarrow a + (-b) \in H$$

Since $a, b \in H \Rightarrow [a + (-b)] \in H$, so H is a subgroup of G.

2-3.22 Theorem: *Let G be an abelian group and H a subset of G consisting of those elements of G which are of the second order, then H is a subgroup of G.*

Proof: By the definition of H,

$$H = \{a \in G : a^2 = e\}$$

Let $a, b \in H$ then $a^2 = e, b^2 = e$.

Next consider

$$(ab^{-1})^2 = (ab^{-1})(ab^{-1}) = a(b^{-1}a)b^{-1}$$
$$= a(ab^{-1})b^{-1} \qquad \because G \text{ is abelian.}$$
$$= (aa)(b^{-1}b^{-1}) = a^2(b^{-1})^2$$
$$= e(b^{-1})^2 \qquad \because a^2 = e$$
$$= (b^{-1})^2 = (b^2)^{-1}$$
$$= e^{-1} = e \qquad \because b^2 = e$$
$$\Rightarrow ab^{-1} \in H$$

Since $a, b \in H \Rightarrow ab^{-1} \in H$, so H is a subgroup of G.

2-3.23 Example: *Let $(Z,+)$ be a group and H a subset of Z consisting of all the multiples of 5, then show that H is a subgroup of G.*

Solution: By the definition of H, $H = \{a \in G : a = 5k, k \in Z\}$

Let $a, b \in H$ then $a = 5k_1, b = 5k_2$, where $k_1, k_2 \in Z$.

Next consider

$$\begin{aligned} a + (-b) &= a - b \\ &= 5k_1 - 5k_2 \\ &= 5(k_1 - k_2) \\ \Rightarrow a + (-b) &\in H \qquad \because (k_1 - k_2) \in Z \end{aligned}$$

Since $a, b \in H \Rightarrow [a + (-b)] \in H$, so H is a subgroup of G.

2-3.24 Example: *Let G be the group of all non-zero complex numbers under multiplication, and let*

$$H = \{a + ib \in G : a^2 + b^2 = 1\}$$

then show that H is a subgroup of G.

PU, 2014 (BS Math)

Solution: Let $x, y \in H$, then

$$x = a + ib, y = c + id, \text{ where } a^2 + b^2 = 1, c^2 + d^2 = 1$$

Next consider

$$\begin{aligned} xy^{-1} &= (a + ib)(c + id)^{-1} \\ &= \frac{a + ib}{c + id} \\ &= \frac{(a + ib)(c - id)}{(c + id)(c - id)} \\ &= \frac{ac + bd + i(bc - ad)}{c^2 + d^2} \\ &= ac + bd + i(bc - ad) \qquad \because c^2 + d^2 = 1 \end{aligned}$$

Now

$$\begin{aligned} (ac + bd)^2 + (bc - ad)^2 &= (a^2 + b^2)(c^2 + d^2) \\ &= 1 \quad \because a^2 + b^2 = 1, c^2 + d^2 = 1 \end{aligned}$$

This shows that $xy^{-1} \in H$. Hence H is a subgroup of G.

2-3.25 Example: *Let H be the set of real numbers $a + b\sqrt{2}$, where $a, b \in Q$ and both are not simultaneously zero. Show that H is a subgroup of the group of non-zero real numbers under multiplication.*

Solution: Let $x, y \in H$, then

$$x = a + b\sqrt{2},\ a, b \in Q, \quad \text{either } a \neq 0 \text{ or } b \neq 0$$

$$\text{and } y = c + d\sqrt{2},\ a, b \in Q, \quad \text{either } c \neq 0 \text{ or } d \neq 0$$

Next consider

$$xy^{-1} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}$$

$$= \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}$$

$$= \left(\frac{ac-2bd}{c^2-2d^2}\right)+\left(\frac{bc-ad}{c^2-2d^2}\right)\sqrt{2}$$

$$\Rightarrow xy^{-1} = a'+b'\sqrt{2}, \text{ where } a' = \left(\frac{ac-2bd}{c^2-2d^2}\right),\ b' = \left(\frac{bc-ad}{c^2-2d^2}\right)$$

Since $a', b' \in Q$ such that $a' \neq 0$ or $b' \neq 0$, so

$$a'+b'\sqrt{2} \in H$$

$$\Rightarrow xy^{-1} \in H$$

This shows that H is a subgroup of G.

2-3.26 Example: *Let H be the set of complex numbers of the form $a+b\sqrt{-5}$, where $a,b \in Q$ and both are not simultaneously zero. Show that H is a subgroup of the group of non-zero complex numbers under multiplication.*

Solution: Let $x, y \in H$, then

$$x = a+b\sqrt{-5},\ a,b \in Q,\quad \text{either } a \neq 0 \text{ or } b \neq 0$$

$$\text{and}\quad y = c+d\sqrt{-5},\ a,b \in Q,\quad \text{either } c \neq 0 \text{ or } d \neq 0$$

Next consider

$$xy^{-1} = \frac{a+b\sqrt{-5}}{c+d\sqrt{-5}} = \frac{(a+b\sqrt{-5})(c-d\sqrt{-5})}{(c+d\sqrt{-5})(c-d\sqrt{-5})}$$

$$= \frac{(ac+5bd)+(bc-ad)\sqrt{-5}}{c^2+5d^2}$$

$$= \left(\frac{ac+5bd}{c^2+5d^2}\right)+\left(\frac{bc-ad}{c^2+5d^2}\right)\sqrt{-5}$$

$$\Rightarrow xy^{-1} = a'+b'\sqrt{-5}, \text{ where } a' = \left(\frac{ac+5bd}{c^2+5d^2}\right),\ b' = \left(\frac{bc-ad}{c^2+5d^2}\right)$$

Since $a', b' \in Q$ such that $a' \neq 0$ or $b' \neq 0$, so

$$a'+b'\sqrt{-5} \in H$$

$$\Rightarrow xy^{-1} \in H$$

This shows that H is a subgroup of G.

2-3.27 Example: *Let H be the set of complex numbers of the form*

$a+b\sqrt{-7}$, where $a,b\in Q$ and both are not simultaneously zero. Show that H is a subgroup of the group of non-zero complex numbers under multiplication.

Solution: Let $x,y\in H$, then

$$x=a+b\sqrt{-7},\ a,b\in Q,\quad \text{either } a\neq 0 \text{ or } b\neq 0$$

$$\text{and}\quad y=c+d\sqrt{-7},\ a,b\in Q,\quad \text{either } c\neq 0 \text{ or } d\neq 0$$

Next consider

$$xy^{-1}=\frac{a+b\sqrt{-7}}{c+d\sqrt{-7}}=\frac{(a+b\sqrt{-7})(c-d\sqrt{-7})}{(c+d\sqrt{-7})(c-d\sqrt{-7})}$$

$$=\frac{(ac+7bd)+(bc-ad)\sqrt{-7}}{c^2+5d^2}$$

$$=\left(\frac{ac+7bd}{c^2+7d^2}\right)+\left(\frac{bc-ad}{c^2+7d^2}\right)\sqrt{-7}$$

$$\Rightarrow xy^{-1}=a'+b'\sqrt{-7},\ \text{where } a'=\left(\frac{ac+7bd}{c^2+7d^2}\right),\ b'=\left(\frac{bc-ad}{c^2+7d^2}\right)$$

Since $a',b'\in Q$ such that either $a'\neq 0$ or $b'\neq 0$, so

$$a'+b'\sqrt{-7}\in H$$

$$\Rightarrow xy^{-1}\in H$$

This shows that H is a subgroup of G.

2-3.28 Theorem: *Let H be the subset of a group G, then H is a subgroup of G if and only if,*

(i) $H^2=H$

(ii) $H^{-1}=H$

Proof: Let H be a subgroup of G, then we have to prove conditions (i) and (ii).

(i) Let $x\in H^2$, then $x=h_1h_2$ for some $h_1,h_2\in H$.

Since H is a subgroup of G, so

$$h_1,h_2\in H$$

$$\Rightarrow h_1h_2\in H$$

$$\Rightarrow x\in H$$

$$\Rightarrow H^2\subset H \qquad \ldots(1)$$

Let $y\in H$. Since H is a subgroup of G, so the identity element is also in H. Let e be the identity element, then

$$e\in H$$

$$\Rightarrow ey\in H^2$$

$$\Rightarrow y\in H^2\Rightarrow H\subset H^2 \qquad \ldots(2)$$

Combining (1) and (2), we get $H^2 = H$.

(ii) Let $x \in H^{-1}$, then $x = h^{-1}$ for some $h \in H$

Since H is a subgroup of G, so

$$h \in H$$
$$\Rightarrow h^{-1} \in H$$
$$\Rightarrow x \in H$$
$$\Rightarrow H^{-1} \subset H \quad \ldots(3)$$

Let $y \in H$ Since H is a subgroup of G, so

$$y \in H$$
$$\Rightarrow y^{-1} \in H$$
$$\Rightarrow (y^{-1})^{-1} \in H^{-1}$$
$$\Rightarrow y \in H^{-1}$$
$$\Rightarrow H \subset H^{-1} \quad \ldots(4)$$

Combining (2) and (3), we get $H^{-1} = H$.

Conversely, suppose that

(i) $H^2 = H$

(ii) $H^{-1} = H$

then we have to show that H is a subgroup of G,. For this let $x, y \in H$, then , by (ii) $y^{-1} \in H$ and by (i) $xy^{-1} \in H$.

This shows that H is a subgroup of G.

2-3.29 Theorem: *If H, K are subgroups of an abelian group G, then HK is a is a subgroup of G.*

PU, 2002 (B.A./B.Sc.)

Proof: Let $x, y \in HK$, then

$$x = h_1k_1, y = h_2k_2 \text{ for some } h_1, h_2 \in H, k_1, k_2 \in K$$

Consider

$$\begin{aligned} xy^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= (h_1k_1)(k_2^{-1}h_2^{-1}) \\ &= h_1(k_1k_2^{-1})h_2^{-1} \\ &= h_1k_3h_2^{-1} \qquad (k_3 = k_1k_2^{-1}) \\ &= h_1h_2^{-1}k_3 \qquad \because G \text{ is abelian} \\ &= h_3k_3 \qquad (h_3 = h_1h_2^{-1}) \end{aligned}$$

Since H and K are subgroups of G, so

$$h_1, h_2 \in H$$
$$\Rightarrow h_3 = h_1h_2^{-1} \in H$$

and $k_1, k_2 \in K$

$\Rightarrow k_3 = k_1 k_2^{-1} \in K$

$\Rightarrow h_3 k_3 \in HK$

$\Rightarrow xy^{-1} \in HK$

This show sthat HK is a subgroup of G.

2-3.30 Example: *If G is a group and a is a fixed element of G, then show that the subset $H = \{x \in G : ax = xa\}$ of G is a subgroup of G.*

PU, 1999 (B.A./B.Sc.)

Solution: Let $x, y \in H$, then by the definition of H,

$$ax = xa \quad \ldots(1)$$

and $$ay = ya \quad \ldots(2)$$

Next consider

$$a(xy^{-1}) = (ax)y^{-1} \text{ (associative law)}$$
$$= (xa)y^{-1} \quad \text{(by (1))}$$
$$= x(ay^{-1}) \text{ (associative law)}$$
$$\Rightarrow a(xy^{-1}) = x(ay^{-1}) \quad \ldots(3)$$
$$(2) \Rightarrow y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$$
$$\Rightarrow y^{-1}a(yy^{-1}) = (y^{-1}y)ay^{-1}$$
$$\Rightarrow y^{-1}ae = eay^{-1}$$
$$\Rightarrow y^{-1}a = ay^{-1}$$

Using this in (3), we get

$$\Rightarrow a(xy^{-1}) = x(y^{-1}a)$$
$$\Rightarrow a(xy^{-1}) = (xy^{-1})a \text{ (associative law)}$$
$$\Rightarrow xy^{-1} \in H$$

Hence H is a subgroup of G.

2-3.31 Example: *Show that every subgroup of an abelian group is abelian.*

Solution: Let G be an abelian group. Let H be a subgroup of G, then we have to show that H is also abelian, for this let $a, b \in H$ then $a, b \in G \quad \because H \subset G$

Since G is abelian, so $ab = ba$. This show sthat H is abelian.

2-3.32 Example: *Let $(G, \cdot)$ be a group and 'a' be a fixed element of G, show that $H = \{a^k : k \in Z\}$ is a subgroup of G.*

Solution: Let $x, y \in H$, then there exist integers m, n such that

$$x = a^m \text{ and } y = a^n$$

Consider

$$xy^{-1} = a^m(a^n)^{-1}$$
$$= a^m a^{-n}$$
$$= a^{m-n} \qquad \because m-n \in Z, \therefore a^{m-n} \in H$$
$$\Rightarrow xy^{-1} \in H$$

This shows that H is a subgroup of G.

2-3.33 Example: *If H is a subgroup of K and K is a subgroup of G, then show that H is a subgroup of G.*

Solution: Since H is a subgroup of K and K is a subgroup of G, so H is a subset of G. For any $x, y \in H, xy^{-1} \in H$, since H is a subgroup of K. Thus, H being the subset of G such that for any $x, y \in H, xy^{-1} \in H$, is a subgroup of G.

2-3.34 Example: *Let $(Z,+)$ be the group of integers. Write two subsets of Z which are closed under addition but are not subgroups of Z.*

Solution: If we take H as a set of positive integers, i.e.

$$H = \{1, 2, 3, \ldots\}$$

and K as a set of non-negative even integers, i.e.

$$K = \{0, 2, 4, \ldots\},$$

then both H and K are closed under addition, but the additive inverses do not exist in these sets. Therefore, both H and K are not subgroups of Z.

2-3.35 Example: *Let H and K be two subgroups of a finite group G. Prove that for any $a \in G$, $a(H \cap K) = aH \cap aK$.*

PU, 1999 (B.A./B.Sc.)

Solution: Since $H \cap K \subset H$ and $H \cap K \subset K$, therefore

$$a(H \cap K) \subset aH \text{ and } a(H \cap K) \subset aK \quad \forall a \in G$$
$$\Rightarrow a(H \cap K) \subset aH \cap aK \qquad \ldots(1)$$

- Let
$$y \in aH \cap aK$$
$$\Rightarrow y \in aH \text{ and } y \in aK$$
$$\Rightarrow a^{-1}y \in H \text{ and } a^{-1}y \in K$$
$$\Rightarrow a^{-1}y \in H \cap K$$
$$\Rightarrow y \in a(H \cap K)$$
$$\Rightarrow aH \cap aK \subset a(H \cap K) \qquad \ldots(2)$$

Combining (1) and (2), we have

$$aH \cap aK = a(H \cap K)$$

2-3.36 Example: *Let H be a subgroup of a group G. If $(Ha)^{-1} = \{(ha)^{-1} : h \in H\}$, then show that $(Ha)^{-1} = a^{-1}H$.*

PU, 2013; 2012 (B.A./B.Sc.)

Solution: Let $x \in (Ha)^{-1}$, then for some $h \in H$,

$$x = (ha)^{-1}$$
$$= a^{-1}h^{-1} \in a^{-1}H \quad \because h^{-1} \in H$$
$$\Rightarrow (Ha)^{-1} \subset a^{-1}H \qquad \ldots(1)$$

Conversely,

let $y \in a^{-1}H$, then for some $h \in H$,

$$y = a^{-1}h$$
$$= (h^{-1}a)^{-1} \in (Ha)^{-1}$$
$$\Rightarrow a^{-1}H \subset (Ha)^{-1} \qquad \ldots(2)$$

Comparing (1) and (2), we have

$$(Ha)^{-1} = a^{-1}H$$

2-3.37 Example: *Let*

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in R,\ ad - bc \neq 0 \right\}$$

be the group of all real 2×2 matrices under matrix multiplication. Show that

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a,b,d \in R,\ ad \neq 0 \right\}$$

is a subgroup of G and

$$K = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in R \right\}$$

is a subgroup of H.

Solution: Let $A, B \in H$, then

$$A = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix},\ B = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}, \text{ where } a_1 d_1 \neq 0,\ a_2 d_2 \neq 0$$

$$\Rightarrow AB^{-1} = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} 1/a_2 & -b_2/a_2 d_2 \\ 0 & 1/d_2 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a_1}{a_2} & \frac{-a_1 b_2}{a_2 d_2} \\ 0 & \frac{d_1}{d_2} \end{bmatrix} \in H \quad \because \frac{a_1}{a_2}\frac{d_1}{d_2} \neq 0$$

This shows that H is a subgroup of G. Let $A, B \in K$, then

$$A=\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix},\ B=\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix}$$

$$\Rightarrow AB^{-1}=\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & -b\\ 0 & 1\end{bmatrix}$$

$$=\begin{bmatrix}1 & a-b\\ 0 & 1\end{bmatrix}\in K$$

This shows that H is a subgroup of G.

2-4 Cyclic Groups

In this section we shall discuss very important type of groups. Some theorems are also presented in this section about this particular type of groups. The concepts of subgroups and the orders of elements are also discussed in the light of this type of groups.

2-4.1 Definition: A group G is said to be *cyclic group* under multiplication if each element of G is a power of one and the same element of G. Such an element of the group is called the *generator of the group*.

If the generator of a cyclic group G is a, then we say that G is a cyclic group generated by a.

If G is a cyclic group of finite order n generated by a, then we write it as

$$G=<a:a^n=e>$$

We read it as "G is a cyclic group of order n generated by a".

2-4.2 Example: *Show that the set of n nth roots of unity is a cyclic group under multiplication.*

Solution:

Let $G=\{1,\omega,\omega^2,...,\omega^{n-1}\}$, where $\omega=e^{\frac{2\pi i}{n}}$, be the set of n nth roots of unity. Since

$$\omega^n=e^{2\pi i}$$
$$=\cos 2\pi+i\sin 2\pi$$
$$=1$$

This shows that each element of G is a power of ω, so G is a cyclic group under multiplication generated by ω.

2-4.3 Example: *If $G=\{\pm 1,\pm i\}$. Show that $(G,\cdot)$ cyclic group and find its generators.*

Solution: Since each element of $G=\{\pm 1,\pm i\}$ is a power of i, so i is a

generator of G. Similarly, each element of G is also a power of $-i$, so $-i$ is also a generator of $-i$. This shows that $(G,\cdot)$ is a cyclic group with $\pm i$ as its generators.

This example also shows that a cyclic group may have two generators.

2-4.4 Definition: A group G is said to be a *cyclic group* under addition generated by a if each element of G is a multiple of a. That is

$$G = \{ka : k \in Z\}$$

2-4.5 Example: Since each integer is a multiple of 1 and -1, therefore $(Z,+)$ is a cyclic group generated by 1 and -1.

2-4.6 Definition: If G is not a cyclic group and H is a subgroup of G such that $H = \{a^n : n \in Z\}$ for some fixed $a \in G$, then H is called the *cyclic subgroup* of G.

2-4.7 Theorem: *Every cyclic group is abelian.*

PU, 2013; 2012 (BS Math)

Proof: Let G be cyclic group generated by a. Let $x, y \in G$, then there exist integers k, m such that

$$x = a^k, \text{ and } y = a^m$$

Consider

$$xy = a^k a^m = a^{k+m} = a^{m+k} = a^m a^k$$
$$= yx$$

This shows that G is an abelian group.

2-4.8 Example: *Show that $(Q,+)$ is an abelian group but not cyclic.*

PU, 2014; 2012 (BS Math)

Solution: Since the commutative law under addition holds in Q, so $(Q,+)$ is an abelian group.

Suppose, if possible, that $(Q,+)$ is a cyclic group generated by a, then all elements of Q must be integral multiples of a. Since a is a generator of set of rational numbers, so a must itself be a rational number. Let

$$a = \frac{p}{q}, \quad p, q \in Z, q \neq 0$$

Since $\frac{1}{2q}$ is a rational number, so it must be an integral multiple of a, i.e. there must exist some integer such that

$$\frac{1}{2q} = na$$

$$\Rightarrow \frac{1}{2q} = n\frac{p}{q}$$

$$\Rightarrow \frac{1}{2} = pn \qquad \ldots(1)$$

Since p, n are integers and the product of two integers is also an integer, so (1) cannot be satisfied for any integral values of p and n. This shows that $\frac{1}{2q}$ is not an integral multiple of a. Hence a is not a generator of Q and, therefore, $(Q,+)$ is not a cyclic group.

2-4.9 Example:

Generate the multiplicative cyclic group by $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Solution: Let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \text{ then}$$

$$A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\Rightarrow A^3 = AA^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$\Rightarrow A^4 = AA^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2-4.10 Theorem: *Every subgroup of a cyclic group is cyclic.*

PU, 2012 (B.A./B.Sc.); PU, 2012 (BS Math)

Proof: Let G be a cyclic group generated by a, then every element of G is a power of a. Let H be the subgroup of G, then we have to show that H is cyclic. Let k be the last positive integer such that $a^k \in H$. Let b be any arbitrary element of H, then b will also be in G. Since G is cyclic, so there must exist an integer m such that $b = a^m$.

Since $a^m = b \in H$ and k is the least positive integer such that $a^k \in H$, so $k \leq m$. Thus, by division algorithm, we have integers q, r such that

$$m = qk + r, \quad 0 \leq r < k \qquad \ldots(1)$$

$$\Rightarrow a^m = a^{qk+r}, \quad 0 \leq r < k$$

$$\Rightarrow a^m = a^{qk}a^r, \quad 0 \leq r < k$$

$$\Rightarrow a^r = a^m a^{-qk}, \quad 0 \leq r < k$$

$$\Rightarrow a^r = a^m(a^k)^{-q}, \quad 0 \leq r < k$$

Since $a^k \in H$ and H is a subgroup of G, so $(a^k)^{-q} \in H$.

$$\Rightarrow a^m (a^k)^{-q} \in H$$

$$\Rightarrow a^r \in H$$

Since $r < k$, so $a^r \in H$ is only possible if $r = 0$. Putting this value in (1), we have $m = qk$. Thus

$$b = a^m = a^{qk} = (a^k)^q$$

This shows that b is a power of a^k. Since b is an arbitrary point of H, so each point is a power of a^k. Hence H is a cyclic subgroup of G generated by a^k.

2-4.11 Theorem: *The order of a cyclic group is equal to the order of its generator.*

Proof: Let G be a cyclic group generated by a. Let n be the order of G. The elements of G are of the form

$$a, a^2, a^3, \ldots, a^{n-1}, a^n$$

If e is the identity element of G, then first of all we show that

$$a^m \neq e \text{ for } m < n$$

For this we suppose on contrary that

$$a^m = e \text{ for some } m < n \qquad \ldots(1)$$

Then

$$a^{m+1} = a, a^{m+2} = a^2, \ldots$$

Thus in the collection

$$a, a^2, a^3, \ldots, a^{n-1}, a^n$$

the elements of G are

$$a, a^2, a^3, \ldots, a^{m-1}, a^m$$

This shows that the order of G is $m < n$ which is contradiction to the fact that the order of G is n. Thus our assumption that

$$a^m = e \text{ for some } m < n$$

is wrong. Consequently

$$a^m \neq e \quad \forall\, m < n \qquad \ldots(2)$$

Next we show that

$$a, a^2, a^3, \ldots, a^{n-1}, a^n$$

are distinct elements of G. For this once again suppose on contrary that there exist integers r, s such that

$$a^r = a^s, \quad 0 < r < s \leq n$$

$$\Rightarrow a^{s-r} = e$$

which is impossible, because $s - r < n$.

Thus $a, a^2, a^3, \ldots, a^{n-1}, a^n$ are distinct elements of G. since these elements

are n in number and the order of G is also n, so the identity element must be one of them. The condition

$$a^m \neq e \quad \forall\ m < n$$

$$\Rightarrow a^n = e$$

This shows that the order of G is n. Hence the order of a cyclic group is same as that of its generator.

2-4.12 Theorem: *An infinite cyclic group has exactly two distinct generators.*

PU, 2015 (BS Math); PU, 2009 (M.Sc. Math)

Proof: Let G be an infinite cyclic group generated by a. Let $x \in G$, then

$$x = a^n \qquad \text{for some } n \in Z$$

$$\Rightarrow x = (a^{-1})^{-n} \qquad \text{for some } n \in Z$$

This shows that each element x of G is also a power of a^{-1}. Hence a^{-1} is also a generator of G. Next we show that $a^{-1} \neq a$. For this suppose on contrary that $a^{-1} = a$, then $a^2 = e$. This shows that the order of a is 2. Since the order of the cyclic group is same as that of its generator, so the order of G is also 2. But G is of infinite order, so $a^{-1} = a$ is wrong. Hence $a^{-1} \neq a$.

Finally suppose that b is also the generator of G such that $b \neq a^{-1}$ and $b \neq a$. Since a and a^{-1} are elements of G and b is its generator, so there must exist integers k and m such that

$$a = b^k \quad \text{and} \quad a^{-1} = b^m$$

$$\Rightarrow a = b^{-m}$$

$$\Rightarrow b^k = a = b^{-m}$$

$$\Rightarrow b^k = b^{-m}$$

$$\Rightarrow b^{k+m} = e$$

This shows that the order of b is $k+m$ which is again impossible, because G is of infinite order, so b is not a generator of G. Hence the infinite cyclic group has exactly two distinct generators.

2-4.13 Theorem: *If G is a cyclic group of order n generated by a, then for each positive divisor d of n, there is a unique subgroup of G of order d.*

PU, 2013 (BS Math)

Proof: Let G be a cyclic group of order n generated by a, i.e.

$$G = \langle a : a^n = e \rangle$$

Let d be a positive divisor of n, then there exists an integer q such that

$$n = qd \qquad \ldots(1)$$

Let $b = a^q$, then

$$b^d = (a^q)^d = a^{qd} = a^n = e$$

This shows that

$$H = < b : b^d = e >$$

is the required subgroup of G.

To see that H is unique, suppose that K is another subgroup of G of order d. Then K is generated by an element $c = a^k$, where k is the least such positive integer. Since d is the order of K, so

$$c^d = e$$
$$\Rightarrow (a^d)^k = e$$
$$\Rightarrow a^{kd} = e, \quad \text{where } kd = n$$
$$\Rightarrow k = \frac{n}{d} = q$$
$$\Rightarrow b = a^q = a^k = c$$

This shows H and K have same generators. Since H and K are cyclic groups of same order having same generator, so $H = K$.

2-4.14 Theorem: *If G is a cyclic group of even order, then there is only one subgroup of G of order 2.*

Proof: Let G be cyclic group of order $2n$, where n is a positive integer, generated by a.

By previous theorem, if a positive integer d divides $2n$, then G has exactly one subgroup of order d. Since 2 divides $2n$, so G has only one subgroup of order 2.

2-4.15 Theorem: *If G is a cyclic group of $4n$, where n is a positive integer, then there is only one subgroup of G of order 4.*

Proof: Let G be cyclic group of order $4n$, where n is a positive integer, generated by a.

By theorem 2-4.14, if a positive integer d divides $4n$, then G has exactly one subgroup of order d. Since 4 divides $4n$, so G has only one subgroup of order 4.

2-4.16 Theorem: *If G is a cyclic group of $3n$, where n is a positive integer, then there is only one subgroup of G of order 3.*

Proof: Let G be cyclic group of order $3n$, where n is a positive integer, generated by a.

By theorem 2-4.14, if a positive integer d divides $3n$, then G has exactly one subgroup of order d. Since 3 divides $3n$, so G has only one subgroup of order 3.

2-4.17 Theorem: *If G is a cyclic group of $6n$, where n is a positive integer, then there is only one subgroup of G of order 3 and only one subgroup of G of order 2.*

Proof: Let G be cyclic group of order $6n$, where n is a positive integer, generated by a.

By theorem 2-4.14, if a positive integer d divides $6n$, then G has exactly one subgroup of order d. Since 2 and 3 divide $6n$, so G has only one subgroup of order 3 and only one subgroup of order 2.

2-5 Lagrange's Theorem and its Applications

The Lagrange's theorem revealed a marvellous result of the finite group theory. It opened the new doors for the study of the finite groups. In this section we shall study the Lagrange's theorem and its applications in finite groups. Some other definitions are also presented in this section which will be helpful in proving the Lagrange's theorem.

2-5.1 Definition:

Let H be a subgroup of a group G and $a \in G$, then the set

$$aH = \{ah : h \in H\}$$

is said to be the *left coset* of H in G determined by a.
Similarly, the set

$$Ha = \{ha : h \in H\}$$

is called the *right coset* of H in G determined by a.

2-5.2 Example: If

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in R, ad - bc \neq 0 \right\}$$

is the group of all real 2×2 matrices under matrix multiplication and

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a,b,d \in R, ad \neq 0 \right\}$$

is a subgroup of G, then for

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in G$$

the set

$$AH = \left\{ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,d \in R, ad \neq 0 \right\}$$

is a left coset of H in G determined by A.
Similarly, the set

$$HA = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} : a,b,d \in R, ad \neq 0 \right\}$$

is a right coset of H in G determined by A.

2-5.3 Example: *If H is a subgroup of a group G, then show that H itself is both left coset and right coset of H in G.*

Solution: Since the identity element e of G is in G such that

$$eH = \{eh : h \in H\} = \{h : h \in H\} = H$$

and

$$He = \{he : h \in H\} = \{h : h \in H\} = H$$

so H is both left and right coset of H in G.

2-5.4 Definition:

If H is a subgroup of $(G,+)$ and $a \in G$, then the set

$$a + H = \{a + h : h \in H\}$$

is said to be the *left coset* of H in G determined by a.

Similarly, the set

$$H + a = \{h + a : h \in H\}$$

is called the *right coset* of H in G determined by a.

2-5.5 Example: Let

$$G = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$$

be the group of residue classes modulo 6 under addition, then

$$H = \{\bar{0},\bar{2},\bar{4}\}$$

is a subgroup of G. The sets

$$\bar{0} + H = H$$

and

$$\bar{1} + H = \{\bar{1},\bar{3},\bar{5}\}$$

are the left costs of H in G.

2-5.6 Definition: A collection $\{A_\alpha : \alpha \in I\}$ of subsets of a set A is called the *partition* of A if

(i) $A = \bigcup_{\alpha \in I} A_\alpha$

(ii) $A_\alpha \cap A_\beta = \phi$ for $\alpha \neq \beta$

2-5.7 Theorem: *Let H be a subgroup of a group G, then the set of all left cosets of H in G defines a partition of G.*

PU, 2002 (B.A./B.Sc.)

Proof: Let

$$\{aH : a \in G\}$$

be the collection of all the left cosets of H in G. For each

$$a \in G, a = ae \in H \quad \because e \in H$$

This shows that

$$G \subset \bigcup_{a \in G} aH \qquad \ldots(1)$$

Since each aH is a subset of G, so

$$\bigcup_{a \in G} aH \subset G \qquad \ldots(2)$$

Combining (1) and (2), we have

$$G = \bigcup_{a \in G} aH \qquad \ldots(3)$$

Next suppose that aH and bH are two distinct left cosets of H in G, then we have to show that their intersection is an empty set. For this suppose on contrary that

$$aH \cap bH \neq \phi$$

Let

$$x \in aH \cap bH$$
$$\Rightarrow x \in aH \quad \text{and} \quad x \in bH$$
$$\Rightarrow x = ah_1, x = bh_2 \text{ for some } h_1, h_2 \in H$$
$$\Rightarrow ah_1 = x = bh_2$$
$$\Rightarrow ah_1 = bh_2$$
$$\Rightarrow a = bh_2h_1^{-1} \quad \text{and} \quad b = ah_1h_2^{-1}$$
$$\Rightarrow a = bh_3, \text{ where } h_3 = h_2h_1^{-1} \in H \because H \text{ is subgroup} \quad \ldots(4)$$
$$\text{and } b = ah_4, \text{ where } h_4 = h_1h_2^{-1} \in H \because H \text{ is subgroup} \quad \ldots(5)$$

Let $y \in aH$ be any arbitrary point of aH, then

$$y = ah_5 \quad \text{for some } h_5 \in H$$
$$= (bh_3)h_5, \quad \text{using (4)}$$
$$= bh_3h_5$$
$$= bh_6 \quad h_6 = h_3h_5 \in H$$
$$\Rightarrow y = bh_6 \in bH$$
$$\Rightarrow aH \subset bH \quad \ldots(6)$$

Let $z \in bH$ be any arbitrary point of bH, then

$$z = bh_7 \quad \text{for some } h_7 \in H$$
$$= (ah_4)h_7, \quad \text{using (5)}$$
$$= ah_4h_7$$
$$= ah_8 \quad h_8 = h_4h_7 \in H$$
$$\Rightarrow z = ah_8 \in aH$$
$$\Rightarrow bH \subset aH \quad \ldots(7)$$

Combining (6) and (7), we have

$$bH = aH$$

which is a contradiction, because aH and bH were distinct. Therefore

$$aH \cap bH = \phi \quad \ldots(8)$$

Relations (3) and (8) show that $\{aH \,.\, a \in G\}$ defines a partition of G. This completes the proof.

2-5.8 Theorem: *Let H be a subgroup of a group G, then the set of all right cosets of H in G defines a partition of G.* PU, 2013 (BS Math)

Proof: Let

$$\{Ha : a \in G\}$$

be the collection of all the right cosets of H in G. For each

$$a \in G, a = ea \in H \quad \because e \in H$$

This shows that

$$G \subset \bigcup_{a \in G} Ha \qquad \ldots(1)$$

Since each Ha is a subset of G, so

$$\bigcup_{a \in G} Ha \subset G \qquad \ldots(2)$$

Combining (1) and (2), we have

$$G = \bigcup_{a \in G} Ha \qquad \ldots(3)$$

Next suppose that Ha and Hb are two distinct right cosets of H in G, then we have to show that their intersection is an empty set. For this suppose on contrary that

$$Ha \cap Hb \neq \phi$$

Let

$$x \in Ha \cap Hb$$

$$\Rightarrow x \in Ha \quad \text{and} \quad x \in Hb$$

$$\Rightarrow x = h_1 a, x = h_2 b \text{ for some } h_1, h_2 \in H$$

$$\Rightarrow h_1 a = x = h_2 b$$

$$\Rightarrow h_1 a = h_2 b$$

$$\Rightarrow a = h_1^{-1} h_2 b \quad \text{and} \quad b = h_2^{-1} h_1 a$$

$$\Rightarrow a = h_3 b, \text{ where } h_3 = h_1^{-1} h_2 \in H \because H \text{ is subgroup} \qquad \ldots(4)$$

$$\text{and } b = h_4 a, \text{ where } h_4 = h_2^{-1} h_1 \in H \because H \text{ is subgroup} \qquad \ldots(5)$$

Let $y \in Ha$ be any arbitrary point of Ha, then

$$y = h_5 a \quad \text{for some } h_5 \in H$$

$$= h_5 (h_3 b), \quad \text{using (4)}$$

$$= h_5 h_3 b$$

$$= h_6 b \quad h_6 = h_5 h_3 \in H$$

$$\Rightarrow y = h_6 b \in Hb$$

$$\Rightarrow Ha \subset Hb \qquad \ldots(6)$$

Let $z \in Hb$ be any arbitrary point of Hb, then

$$z = h_7 b \quad \text{for some } h_7 \in H$$

$$= h_7 (h_4 a), \quad \text{using (5)}$$

$$= h_7 h_4 a$$

$$= h_8 a \quad h_8 = h_7 h_4 \in H$$

$$\Rightarrow z = h_8 a \in Ha$$

$$\Rightarrow Hb \subset Ha \qquad \ldots(7)$$

Combining (6) and (7), we have

$$Hb = Ha$$

which is a contradiction, because Hb and Hb were distinct.
Therefore

$$Ha \cap Hb = \phi \qquad \ldots(8)$$

Relations (3) and (8) show that

$$\{Ha : a \in G\}$$

defines a partition of G. This completes the proof.

2-5.9 Definition: The number of left (or right) cosets of a subgroup H of a group G is called the *index* of H in G and is denoted by $[G : H]$.

PU, 2014 (BS Math)

2-5.10 Theorem: *In an abelian group every left coset is equal to the corresponding right coset.*

Proof: Let G be an abelian group. Let H be a subgroup of G. Let $a \in G$, then

$$aH = \{ah : h \in H\} \qquad \ldots(1)$$

and

$$Ha = \{ha : h \in H\} \qquad \ldots(2)$$

Since

$$h \in H \subset G \Rightarrow h \in G$$

and G is abelian, therefore

$$ah = ha \quad \forall h \in H$$

This shows that

$$\{ah : h \in H\} = \{ha : h \in H\}$$

$$\Rightarrow aH = Ha$$

This completes the proof.

2-5.11 Theorem: *Let H be a subgroup of a group G, then the number of left cosets is equal to the number of right cosets of H in G.*

Proof: Let

$$R = \{Ha : a \in G\}$$

be the set of all right cosets of H in G and

$$L = \{aH : a \in G\}$$

the set of all left cosets of H in G.

In order to show to that R and L have same number of elements, we shall prove that there exists a bijective mapping from R to L. For this let us consider a mapping $\phi : R \to L$ defined as

$$\phi(Ha^{-1}) = aH$$

Since each element aH of L is an image of some element Ha^{-1} of R under ϕ, so ϕ is onto. Next we show that ϕ is one-one, for this let

$$\phi(Ha^{-1}) = \phi(Hb^{-1}) \Rightarrow aH = bH \Rightarrow H = a^{-1}bH \Rightarrow a^{-1}b \in H$$

$$\Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow H = Hb^{-1}a \Rightarrow Ha^{-1} = Hb^{-1}$$

This shows that ϕ is one-one, therefore ϕ is bijective. Thus the number of members of R is equal to the number of members of L. This completes the proof.

2-5.12 Lagrange's Theorem: *The index and the order of a subgroup of a finite group divide the order of the group.*

PU, 2011; 2010 (B.A./B.Sc.); PU, 2014; 2012 (BS Math); PU, S2014 (M.Sc. Math)

Proof: Let G be a finite group of order n. Let H be a subgroup of G of order m. Since the order of G is finite, so the set

$$\{a_1H, a_2H, \ldots, a_kH\}$$

of all the distinct left cosets of H in G is also finite.

Consider the mapping

$$\phi : H \to a_iH$$

defined as

$$\phi(h) = a_ih,\ h \in H$$

Since each element $a_ih \in a_iH$ is an image of some element $h \in H$ under ϕ, so ϕ is onto.

Next consider

$$\phi(h_1) = \phi(h_2),\ \ h_1, h_2 \in H$$
$$\Rightarrow a_ih_1 = a_ih_2$$
$$\Rightarrow h_1 = h_2$$

This shows that ϕ is one-one. Hence ϕ is bijective. Thus the number of elements in H and in $a_iH\ (1 \le i \le k)$ is the same. Since H has m elements, so each $a_iH\ (1 \le i \le k)$ also has m elements.

Since the left cosets define the partition of G, so

$$G = \bigcup_{i=1}^{k} a_iH$$

and $$a_iH \cap a_jH = \phi \quad i \neq j\ 1 \le i, j \le k$$

This shows that

$$|G| = \sum_{i=1}^{k} |a_iH|$$

$$\Rightarrow n = |a_1H| + |a_2H| + \ldots + |a_kH| \qquad \because |G| = n$$
$$= m + m + \ldots + m \qquad \because |a_iH| = m, 1 \le i \le n$$
$$= km$$
$$\Rightarrow n = km \qquad \ldots(1)$$

(1) shows that both k and m divides n. Since k, being the number of left cosets of H in G, is the index of H in G and m is the order of H. Thus both the index k and the order m of the subgroup H of a finite group G divides the order of the group G.

2-5.13 Example: *Find all the subgroups of the cyclic group of order 24.*
Solution: Let G be a cyclic group of order 24 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24. Thus the required subgroups of G are of orders 1, 2, 3, 4, 6, 8, 12 and 24.
The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 2 is

$$H_2 = \{e, a^{12}\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^8, a^{16}\}$$

The subgroup of order 4 is

$$H_4 = \{e, a^6, a^{12}, a^{18}\}$$

The subgroup of order 6 is

$$H_6 = \{e, a^4, a^8, a^{12}, a^{16}, a^{20}\}$$

The subgroup of order 8 is

$$H_8 = \{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}\}$$

The subgroup of order 12 is

$$H_{12} = \{e, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}, a^{20}, a^{22}\}$$

The subgroup of order 24 is

$$H_{24} = G = \{e, a, a^2, \ldots, a^{22}, a^{23}\}$$

2-5.14 Example: *Find all the subgroups of the cyclic group of order 99.*
Solution: Let G be a cyclic group of order 99 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 99 are 1, 3, 9, 11, 33, and 99. Thus the required subgroups of G are of orders 1, 3, 9, 11, 33, and 99.
The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^{33}, a^{66}\}$$

The subgroup of order 9 is

$$H_9 = \{e, a^{11}, a^{22}, a^{33}, a^{44}, a^{55}, a^{66}, a^{77}, a^{88}\}$$

The subgroup of order 11 is

$$H_{11} = \{e, a^9, a^{18}, a^{27}, a^{36}, a^{45}, a^{54}, a^{63}, a^{72}, a^{81}, a^{90}\}$$

The subgroup of order 33 is

$$H_{33} = \{e, a^3, a^6, a^9, a^{12}, \ldots, a^9, a^{93}, a^{96}\}$$

The subgroup of order 99 is

$$H_{99} = G = \{e, a, a^2, \ldots, a^{97}, a^{98}\}$$

2-5.15 Example: *Find all the subgroups of the cyclic group of order 12.* PU, 2013 (BS Math)

Solution: Let G be a cyclic group of order 12 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 12 are 1, 2, 3, 4, 6, and 12. Thus the required subgroups of G are of orders 1, 2, 3, 4, 6, and 12.

The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 2 is

$$H_2 = \{e, a^6\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^4, a^8\}$$

The subgroup of order 4 is

$$H_4 = \{e, a^3, a^6, a^9\}$$

The subgroup of order 6 is

$$H_6 = \{e, a^2, a^4, a^6, a^8, a^{10}\}$$

The subgroup of order 12 is

$$H_{12} = G = \{e, a, a^2, \ldots, a^{10}, a^{11}\}$$

2-5.16 Example: *Find all the subgroups of the cyclic group of order 21.*

Solution: Let G be a cyclic group of order 21 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 21 are 1, 3, 7, 21. Thus the required subgroups of G are of orders 1, 3, 7, 21. The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^7, a^{14}\}$$

The subgroup of order 7 is

$$H_7 = \{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}\}$$

The subgroup of order 21 is

$$H_{21} = G = \{e, a, a^2, \ldots, a^{19}, a^{20}\}$$

2-5.17 Example: *Find all subgroups of the cyclic group of order 18 generated by a.*

Solution: Let G be a cyclic group of order 18 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order

of G. Now the positive divisors of 18 are 1, 2, 3, 6, 9, 18. Thus the required subgroups of G are of orders 1, 2, 3, 6, 9, 18. The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 2 is

$$H_2 = \{e, a^9\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^6, a^{12}\}$$

The subgroup of order 6 is

$$H_6 = \{e, a^3, a^6, a^9, a^{12}, a^{15}\}$$

The subgroup of order 9 is

$$H_9 = \{e, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}\}$$

The subgroup of order 18 is

$$H_{18} = G = \{e, a, a^2, ..., a^{16}, a^{17}\}$$

2-5.18 Example: *Find all subgroups of the cyclic group of order* 60 *generated by a.*

Solution: Let G be a cyclic group of order 60 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60. Thus the required subgroups of G are of orders 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60.

The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 2 is

$$H_2 = \{e, a^{30}\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^{20}, a^{40}\}$$

The subgroup of order 4 is

$$H_4 = \{e, a^{15}, a^{30}, a^{45}\}$$

The subgroup of order 5 is

$$H_5 = \{e, a^{12}, a^{24}, a^{36}, a^{48}\}$$

The subgroup of order 6 is

$$H_6 = \{e, a^{10}, a^{20}, a^{30}, a^{40}, a^{50}\}$$

The subgroup of order 10 is

$$H_{10} = \{e, a^6, a^{12}, a^{18}, a^{24}, a^{30}, a^{36}, a^{42}, a^{48}, a^{54}\}$$

The subgroup of order 12 is

$$H_{12} = \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, a^{40}, a^{45}, a^{50}, a^{55}\}$$

The subgroup of order 15 is

$$H_{15} = \{e, a^4, a^8, a^{12}, ..., a^{52}, a^{56}\}$$

The subgroup of order 20 is

$$H_{20} = \{e, a^3, a^6, a^9, ..., a^{54}, a^{57}\}$$

The subgroup of order 30 is

$$H_{30} = \{e, a^2, a^4, a^6, ..., a^{56}, a^{58}\}$$

The subgroup of order 60 is

$$H_{60} = G = \{e, a, a^2, ..., a^{58}, a^{59}\}$$

2-5.19 Example: *Find all subgroups of the cyclic group of order 81 generated by a.*

Solution: Let G be a cyclic group of order 81 generated by a. Then, by Lagrange's theorem, the orders of subgroups of G must divide the order of G. Now the positive divisors of 81 are 1, 3, 9, 27, and 81. Thus the required subgroups of G are of orders 1, 3, 9, 27, and 81.

The subgroup of order 1 is

$$H_1 = \{e\}$$

The subgroup of order 3 is

$$H_3 = \{e, a^{27}, a^{54}\}$$

The subgroup of order 9 is

$$H_9 = \{e, a^9, a^{18}, a^{27}, a^{36}, a^{45}, a^{54}, a^{63}, a^{72}\}$$

The subgroup of order 27 is

$$H_{27} = \{e, a^3, a^6, a^9, ..., a^{75}, a^{78}\}$$

The subgroup of order 81 is

$$H_{81} = G = \{e, a, a^2, ..., a^{79}, a^{80}\}$$

2-5.20 Theorem: *The order of an element of a finite group divides the order of the group.*

PU, 2012 (BS Math)

Proof: Let G be a group of finite order n. Let a be any arbitrary element of G. Let m be the order of a, then we have to show that m divides n.

We can generate a cyclic subgroup of G by a. Let H be a cyclic subgroup of G generated by a. Since the order of the generator of a cyclic group is equal to the order of its generator. Therefore, m, being the order of a, is the order of H. By Lagrange's theorem m, being the order of the subgroup H of a finite group G, divides the order of G. That is m divides n. Hence the order of an element of a finite group divides the order of the group.

2-5.21 Theorem: *Any group of prime order is cyclic.*

Proof: Let G be a group of prime order p, then we have to show that G is cyclic. Let a be any non-identity element of G. Let H be a cyclic subgroup of G generated by a, then by Lagrange's theorem the order of H must divide the order p of G. Since p is prime, so the order of H is either 1 or p.

But a is non-identity, so the order of H will not be 1. Therefore the order of H is p. This shows that

$$H = G$$

but the G is cyclic, because H is cyclic. Hence any group of prime order is cyclic.

2-5.22 Theorem: *Any group of prime order has no non-trivial subgroups.*
Proof: Let G be a group of prime order p, then we have to show that G has no non-trivial subgroup. For this suppose on contrary that H is a non-trivial subgroup of G. Then

$$H \neq \{e\} \text{ and } H \neq G$$

Let n be the order of H, then by Lagrange's theorem n must divide p. Since p is prime, so either $n = 1$ or $n = p$.

1. If $n = 1$, then $H = \{e\}$.
2. If $n = p$, then $H = G$.

Since both cases lead to a contradiction, so our assumption that H is a non-trivial subgroup of G is wrong. This shows that G has no non-trivial subgroup. Hence a group of prime order has no non-trivial subgroup.

2-5.23 Example: *If a is an element of a group G, then show that $a^{|G|} = e$.*
Solution: Let n be the order of the group G. Let m be the order of an element a of G, then

$$a^m = e \qquad \ldots(1)$$

Let H be a cyclic subgroup of G generated by a. Since the order of the cyclic group is equal to the order of its generator, so m is the order of H. By Lagrange's theorem m, being the order of subgroup H of G, divides the order n of G. Therefore, there must exist an integer q such that

$$n = mq \qquad \ldots(2)$$

Consider

$$\begin{aligned} a^{|G|} &= a^n \quad \because |G| = n \\ &= a^{mq} \quad \text{by (2)} \\ &= (a^m)^q \\ &= e^q \quad \text{by (1)} \\ &= e \end{aligned}$$

$$\Rightarrow a^{|G|} = e$$

2-5.24 Example: *Let G be a cyclic group of order 24 generated by a. Find the orders of the elements* (i) e, (ii) a^9, (iii) a^{10}.

Since $e^1 = e$, so $o(e) = 1$.

Since given cyclic group G is 24 and a is its generator, so

$$a^{24} = e \qquad \ldots(1)$$

(ii) To find the order of a^9, we shall find the least common multiple of 9 and 24. Since 72 is the least common multiple of 9 and 24, so consider

$$\begin{aligned}(a^9)^8 &= a^{72}\\ &= (a^{24})^3\\ &= e^3 \quad \because a^{24} = e\\ &= e\end{aligned}$$

$$\Rightarrow o(a^9) = 8$$

(iii) To find the order of a^{10}, we shall find the least common multiple of 10 and 24. Since 120 is the least common multiple of 10 and 120, so consider

$$\begin{aligned}(a^{10})^{12} &= a^{120}\\ &= (a^{24})^5\\ &= e^5 \quad \because a^{24} = e\\ &= e\end{aligned}$$

$$\Rightarrow o(a^{10}) = 12$$

2-5.25 Example: *If H and K are two finite subgroups of a group G with relatively prime orders, then show that $H \cap K = \{e\}$.*

PU, 2003; 2001 (B.A./B.Sc.)

Solution: Let $o(H) = m$ and $o(K) = n$. Since H and K are of relatively prime orders, so the greatest common divisor of m and n is 1. Since

$$H \cap K \subset H \qquad \ldots(1)$$

and

$$H \cap K \subset K \qquad \ldots(2)$$

Since H, K are subgroups and the intersection of two subgroups is also a subgroup, so (1) and (2) show that $H \cap K$ is a subgroup of both H and K. If k is the order of $H \cap K$, then by Lagrange's theorem, k must divide both orders of H and K. That is k must divide both m and n. But the greatest common divisor of m and n is 1, so

$$k = 1$$

$$\Rightarrow o(H \cap K) = 1$$

$$\Rightarrow H \cap K = \{e\}$$

2-5.26 Example: *Explain why a group of order 47 cannot have proper subgroups.*

Solution: Since 47 is a prime and a group of prime order cannot have a proper subgroup.

In other words if H is a proper subgroup of G, then the order of H is neither 1 nor 47 and any other integer cannot divide 47 contradicting the Lagrange's theorem, therefore a group of order 47 cannot have proper subgroup.

2-5.27 Example: *Let G be a group of order 89. Can G have a non-trivial subgroup?*

Solution: Since 89 is a prime and a group of prime order cannot have a proper subgroup.

In other words if H is a proper subgroup of G, then the order of H is neither 1 nor 89 and any other integer cannot divide 89 contradicting the Lagrange's theorem, therefore a group of order 89 cannot have proper subgroup.

EXERCISE 2

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) The unary operation is an operation which yields another number when performed on

(a) two numbers (b) a single number
(c) three numbers (d) four numbers

ⓐ ⓑ ⓒ ⓓ

(ii) The negation of a given number is a

(a) binary operation (b) relation
(c) unary operation (d) relation in some set

ⓐ ⓑ ⓒ ⓓ

(iii) The extraction of square root of a given number is a

(a) binary operation (b) relation
(c) unary operation (d) relation in some set

ⓐ ⓑ ⓒ ⓓ

(iv) The extraction of cube root of a given number is a

(a) binary operation (b) relation
(c) unary operation (d) relation in some set

ⓐ ⓑ ⓒ ⓓ

(v) The squaring a given number is a

(a) relation in some set (b) relation
(c) binary operation (d) unary operation

ⓐ ⓑ ⓒ ⓓ

(vi) Which of the following is unary operation?

(a) addition (b) multiplication

(c) square root (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vii) If for all $a,b \in A$, $a * b \in A$, then

(a) $*$ is a unary operation in A (b) $a * b = b * a$

(c) $*$ is a binary operation in A (d) $a * b \neq b * a$

ⓐ ⓑ ⓒ ⓓ

(viii) $*$ is said to be commutative in A if for all $a,b \in A$

(a) $a + b = b + a$ (b) $a * b = b * a$

(c) $a - b = b - a$ (d) $a * b \neq b * a$

ⓐ ⓑ ⓒ ⓓ

(ix) If $*$ is a binary operation in A then

(a) A is closed under $*$ (b) A is not closed under $*$

(c) A is closed under + (d) A is closed under –

ⓐ ⓑ ⓒ ⓓ

(x) An element $e \in A$ is said to be the identity element with respect to a binary operation $*$ on A if for all $a \in A$

(a) $e * a = a * e = 0$ (b) $e * a = a * e \neq a$

(c) $e * a = a * e = e$ (d) $e * a = a * e = a$

ⓐ ⓑ ⓒ ⓓ

(xi) The intersection of two subsets A and B of X is

(a) a non-commutative binary operation on $P(X)$

(b) a commutative binary operation on $P(X)$

(c) not a binary operation on $P(X)$

(d) not a member of $P(X)$ ⓐ ⓑ ⓒ ⓓ

(xii) The identity element of a set X with respect to intersection in $P(X)$ is

(a) X (b) ϕ (c) does not exist (d) 0

ⓐ ⓑ ⓒ ⓓ

(xiii) The identity element of a set X with respect to union in $P(X)$ is

(a) X (b) ϕ (c) does not exist (d) 0

ⓐ ⓑ ⓒ ⓓ

(xiv) The union of two subsets A and B of X is

(a) a non-commutative binary operation on $P(X)$

(b) a commutative binary operation on $P(X)$

(c) not a binary operation on $P(X)$

(d) not a member of $P(X)$ ⓐ ⓑ ⓒ ⓓ

(xv) The union of two subsets A and B of X is

(a) a non-commutative binary operation on $P(X)$

(b) an associative binary operation on $P(X)$

(c) not a binary operation on $P(X)$

(d) not a member of $P(X)$ ⓐ ⓑ ⓒ ⓓ

(xvi) In the group $(G,*)$, $\forall a,b \in G$

(a) $a+b \in G$ (b) $ab \in G$

(c) $a*b \in G$ (d) $a-b \in G$

ⓐ ⓑ ⓒ ⓓ

(xvii) If $(G,*)$ is a group then for all $a \in G$ there exists $a' \in G$ such that

(a) $a*a'=0=a'*a$ (b) $a*a'=a'=a'*a$

(c) $a*a'=a=a'*a$ (d) $a*a'=e=a'*a$

ⓐ ⓑ ⓒ ⓓ

(xviii) $(G,*)$ is a commutative or abelian group if for all $a,b \in G$

(a) $a*b=b*a$ (b) $a*b \neq b*a$

(c) $a+b=b*a$ (d) $a*b=b+a$

ⓐ ⓑ ⓒ ⓓ

(xix) Z is a group under

(a) subtraction (b) division

(c) multiplication (d) addition

ⓐ ⓑ ⓒ ⓓ

(xx) The action of wearing socks and shoes

(a) do not commute (b) commute

(c) does not exit (d) is associative

ⓐ ⓑ ⓒ ⓓ

Q.2

(i) The set of all non-singular matrices of order 2 forms a non-abelian group under

(a) addition (b) subtraction

(c) multiplication (d) division

ⓐ ⓑ ⓒ ⓓ

(ii) $\{3^n : n \in Z\}$ is an abelian group under

(a) addition (b) subtraction

(c) multiplication (d) division

ⓐ ⓑ ⓒ ⓓ

(iii) $\{3n : n \in Z\}$ is an abelian group under

(a) addition (b) subtraction

(c) multiplication (d) division

ⓐ ⓑ ⓒ ⓓ

(iv) A monoid is always a

(a) a group (b) a commutative group

(c) a non-abilian group (d) groupoid

ⓐ ⓑ ⓒ ⓓ

(v) A monoid is always a

(a) a group (b) a commutative group

(c) a non-abilian group (d) semi-group

ⓐ ⓑ ⓒ ⓓ

(vi) A semi-group is always a

(a) a group (b) a commutative group

(c) groupoid (d) a non-abilian group

ⓐ ⓑ ⓒ ⓓ

(vii) A closed set with respect to some binary operation is called the
(a) a group (b) a commutative group
(c) groupoid (d) a non-abilian group
ⓐ ⓑ ⓒ ⓓ

(viii) A non-empty set which is closed with respect to some binary operation is called the semi-group if
(a) the binary operation is associative
(b) the binary operation is commutative
(c) the binary operation is anti-commutative
(d) identity element exists
ⓐ ⓑ ⓒ ⓓ

(ix) A non-empty set which is closed with respect to some associative binary operation is called the monoid if
(a) inverse of each element exists
(b) the binary operation is commutative
(c) the binary operation is anti-commutative
(d) identity element exists
ⓐ ⓑ ⓒ ⓓ

(x) $\{-3n : n \in Z\}$ is an abelian group under
(a) addition (b) subtraction (c) multiplication (d) division
ⓐ ⓑ ⓒ ⓓ

(xi) If $G = \{1, -1, i, -i\}$ is a group under multiplication, then inverse of i is
(a) 1 (b) -1 (c) i (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xii) If a, b are elements of a group G, then $(ab)^{-1} =$
(a) $a^{-1}b^{-1}$ (b) $b^{-1}a^{-1}$ (c) $a^{-1}b$ (d) $b^{-1}a$
ⓐ ⓑ ⓒ ⓓ

(xiii) If a, b are elements of a group G, then $(ab^{-1})^{-1} =$
(a) $a^{-1}b^{-1}$ (b) ba^{-1} (c) $a^{-1}b$ (d) $b^{-1}a$
ⓐ ⓑ ⓒ ⓓ

(xiv) If a, b are elements of a group G, then $(a^{-1}b)^{-1} =$
(a) $a^{-1}b^{-1}$ (b) ba^{-1} (c) $a^{-1}b$ (d) $b^{-1}a$
ⓐ ⓑ ⓒ ⓓ

(xv) If a, b are elements of a group G, then $(b^{-1}a^{-1})^{-1} =$
(a) ab (b) ba^{-1} (c) $a^{-1}b$ (d) $b^{-1}a$
ⓐ ⓑ ⓒ ⓓ

(xvi) If $* : X \times X \to X$ is a binary operation, then for all $x, y \in X$, $(x, y) =$
(a) $x \times y$ (b) $x - y$ (c) $x + y$ (d) $x * y$
ⓐ ⓑ ⓒ ⓓ

(xvii) The identity element of the set of integers with respect to + is
(a) 3 (b) 2 (c) 1 (d) 0
ⓐ ⓑ ⓒ ⓓ

(xviii) The identity element of the set of integers with respect to multiplication is
(a) 3 (b) 2 (c) 1 (d) 0
ⓐ ⓑ ⓒ ⓓ

(xix) The group $(G,*)$ is said to be an abelian group or commutative group if for all $a,b \in G$, $a*b =$
(a) $b \div a$ (b) $b-a$ (c) $b+a$ (d) $b*a$
ⓐ ⓑ ⓒ ⓓ

(xx) The set of integers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

Q.3

(i) The set of real numbers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(ii) The set of rational numbers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(iii) The set of complex numbers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(iv) The set of even integers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(v) The set of nonzero real numbers is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(vi) The set $G = \{1, \omega, \omega^2\}$, ω is the cube root of unity, is an abelian group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(vii) The set $C_4 = \{\pm 1, \pm i\}$ of all the fourth roots of unity is a group under the usual
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(viii) The set G of all non-singular matrices of order 2 is a non-abelian group under matrix
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(ix) The set of all those complex numbers whose module are 1 is group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(x) The set $G = \{2^k : k \in Z\}$ is a group under
(a) addition (b) multiplication (c) division (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xi) The set of all n, nth roots of unity forms a group under the _____ of complex numbers.

(a) addition (b) multiplication (c) division (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xii) For any three elements a, b, c of a group G, $ab = ac \Rightarrow$

(a) $a = b$ (b) $a = c$ (c) $b = c$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xiii) For any three elements a, b, c of a group G, $ba = ca \Rightarrow$

(a) $a = b$ (b) $a = c$ (c) $b = c$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xiv) The multiplicative identity element is

(a) $\int_0^4 dx$ (b) $\int_0^3 dx$ (c) $\int_0^2 dx$ (d) $\int_0^1 dx$

ⓐ ⓑ ⓒ ⓓ

(xv) The multiplicative identity element is

(a) $\int_1^4 dx$ (b) $\int_1^3 dx$ (c) $\int_1^2 dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xvi) The multiplicative identity element is

(a) $\int_0^{\frac{\pi}{2}} \cos x dx$ (b) $1 + \int_0^{\frac{\pi}{2}} \cos x dx$ (c) $1 + \int_0^{\frac{\pi}{2}} \sin x dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xvii) The multiplicative identity element is

(a) $1 + \int_0^{\frac{\pi}{2}} \cos x dx$ (b) $\int_0^{\frac{\pi}{2}} \sin x dx$

(c) $1 + \int_0^{\frac{\pi}{2}} \sin x dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xviii) The multiplicative inverse of 2 is

(a) $\int_0^1 x dx$ (b) $\int_0^1 x^2 dx$ (c) $\int_0^1 x^4 dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xix) The multiplicative inverse of 3 is

(a) $\int_0^1 x dx$ (b) $\int_0^1 x^2 dx$ (c) $\int_0^1 x^4 dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xx) The multiplicative inverse of 4 is

(a) $\int_0^1 x dx$ (b) $\int_0^1 x^2 dx$ (c) $\int_0^1 x^4 dx$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

Q.4

(i) In a group $(Z,+)$, the inverse of 7 is

(a) $\begin{vmatrix} 7 & 8 \\ 1 & 1 \end{vmatrix}$ (b) $\begin{vmatrix} 2 & 3 \\ 1 & 3 \end{vmatrix}$ (c) $\begin{vmatrix} 2 & 13 \\ 1 & 3 \end{vmatrix}$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(ii) In a group $(Z,+)$, the inverse of -3 is

(a) $\frac{d}{dx}(2-3x)$ (b) $\frac{d}{dx}(3x-2)$

(c) $\frac{d}{dx}(3)$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(iii) An element a of a group G is said to be idempotent if $a^2 =$

(a) e (b) a (c) a^3 (d) none of these

ⓐ ⓑ ⓒ ⓓ

(iv) If G is a group, then for all $a \in G$, $(a^{-1})^{-1} =$

(a) e (b) a^{-1} (c) a^2 (d) a

ⓐ ⓑ ⓒ ⓓ

(v) If G is a group, then for all $a,b,c \in G$, $(abc)^{-1} =$

(a) $c^{-1}b^{-1}a^{-1}$ (b) $a^{-1}b^{-1}c^{-1}$ (c) cba (d) abc

ⓐ ⓑ ⓒ ⓓ

(vi) For any element a of a group G, $(a^{-1})^n =$

(a) a^n (b) a^{-n} (c) na (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vii) If G is abelian group then for all $a,b \in G$, $(ab)^2 =$

(a) a^2b (b) a^3b^3 (c) a^2b^2 (d) ab

ⓐ ⓑ ⓒ ⓓ

(viii) If G is an abelian group then for all $a,b \in G, n \in Z$, $(ab)^n =$

(a) ab (b) a^nb (c) ab^n (d) a^nb^n

ⓐ ⓑ ⓒ ⓓ

(ix) If G is an abelian group then for all $a,b \in G, n \in Z$, $(ab)^{n+1} =$

(a) ab (b) a^nb (c) ab^n (d) $a^{n+1}b^{n+1}$

ⓐ ⓑ ⓒ ⓓ

(x) The number of elements in a group G is called the _____ of group G.

(a) generator (b) order (c) subgroup (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xi) If a group consists of _____ elements then it is said to be an infinite group.

(a) two (b) three

(c) finite number of (d) infinite number of

ⓐ ⓑ ⓒ ⓓ

(xii) If G is a group and $a \in G$, the order or period of a is the least positive integer n such that $a^n =$

(a) a^3 (b) a^2 (c) a (d) e ⓐ ⓑ ⓒ ⓓ

(xiii) In the group $G=\{-1,1,-i,i\}$, the order of 1 is
(a) -1 (b) 1 (c) 2 (d) 4 ⓐ ⓑ ⓒ ⓓ

(xiv) In the group $G=\{-1,1,-i,i\}$, the order of -1 is
(a) -1 (b) 1 (c) 2 (d) 4 ⓐ ⓑ ⓒ ⓓ

(xv) In the group $G=\{-1,1,-i,i\}$, the order of i is
(a) -1 (b) 1 (c) 2 (d) 4 ⓐ ⓑ ⓒ ⓓ

(xvi) In the group $G=\{-1,1,-i,i\}$, the order of $-i$ is
(a) -1 (b) 1 (c) 2 (d) 4 ⓐ ⓑ ⓒ ⓓ

(xvii) In a group, the order of an element is
(a) less than the order of its inverse
(b) greater than the order of its inverse
(c) same as that of its inverse
(d) none of these ⓐ ⓑ ⓒ ⓓ

(xviii) For an element 'a' of a group,
(a) $o(a) > o(a^{-1})$ (b) $o(a) = o(a^{-1})$
(c) $o(a) < o(a^{-1})$ (d) $o(a) \neq o(a^{-1})$ ⓐ ⓑ ⓒ ⓓ

(xix) In a group G, for all $a,b \in G$,
(a) $o(ab) > o(ba)$ (b) $o(ab) < o(ba)$
(c) $o(ab) = o(ba)$ (d) $o(ab) \neq o(ba)$ ⓐ ⓑ ⓒ ⓓ

(xx) In a group G, for all $\{\pm 1, \pm i\}$,
(a) $o(a) = o(bab^{-1})$ (b) $o(a) < o(bab^{-1})$
(c) $o(a) > o(bab^{-1})$ (d) $o(a) \neq o(bab^{-1})$ ⓐ ⓑ ⓒ ⓓ

Q.5

(i) If in a group G, $b = x^{-1}ax$, then $b^2 =$
(a) $x^{-1}ax$ (b) $x^{-1}a^2x$ (c) $x^{-1}a^3x$ (d) $x^{-1}a^4x$ ⓐ ⓑ ⓒ ⓓ

(ii) If in a group G, $b = x^{-1}a^2x$, then $b^2 =$
(a) $x^{-1}ax$ (b) $x^{-1}a^2x$ (c) $x^{-1}a^3x$ (d) $x^{-1}a^4x$ ⓐ ⓑ ⓒ ⓓ

(iii) If in a group G, $xa = ax$, then $xa^2 =$
(a) a^5x (b) a^4x (c) a^3x (d) a^2x ⓐ ⓑ ⓒ ⓓ

(iv) If in a group G, $xa = ax$, then $xa^3 =$

(a) a^5x (b) a^4x (c) a^3x (d) a^2x

ⓐ ⓑ ⓒ ⓓ

(v) A subset H of a group G is called the _____ of G if H itself is a group under the same binary operation as defined in G.

(a) subspace (b) subgroup (c) subbase (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vi) The set $\{\pm 1\}$ is a subgroup of $\{\pm 1, \pm i\}$ under complex

(a) addition (b) subtraction (c) multiplication (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vii) Let $(G,\cdot)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a, b \in H$, the element

(a) $a + b^{-1} \in H$ (b) $ab^{-1} \notin H$

(c) $a + (-b) \in H$ (d) $ab^{-1} \in H$

ⓐ ⓑ ⓒ ⓓ

(viii) Let $(G,+)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a, b \in H$, the element

(a) $a + (-b) \notin H$ (b) $ab^{-1} \notin H$

(c) $a + (-b) \in H$ (d) $ab^{-1} \in H$

ⓐ ⓑ ⓒ ⓓ

(ix) The intersection of any collection of subgroups of a group G is _____ of G.

(a) not a subgroup (b) a subgroup

(c) a subspace (d) none of these

ⓐ ⓑ ⓒ ⓓ

(x) Every subgroup of an abelian group is

(a) non-abelian (b) cyclic

(c) abelian (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xi) The set of n nth roots of unity is a cyclic group under

(a) multiplication (b) addition

(c) subtraction (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xii) The generators of $G = \{\pm 1, \pm i\}$ are

(a) ± 1 (b) ± 2 (c) $\pm i$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xiii) $(Z,+)$ is a cyclic group generated by

(a) ± 1 (b) ± 2 (c) $\pm i$ (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xiv) Every cyclic group is

(a) non abelian (b) abelian

(c) non commutative (d) none of these

ⓐ ⓑ ⓒ ⓓ

(xv) Every subgroup of a cyclic group is
(a) non abelian (b) non cyclic
(c) cyclic (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xvi) Order of a cyclic group is _____ the order of its generator.
(a) equal to (b) less than (c) greater than (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xvii) An infinite cyclic group has exactly _____ distinct generators.
(a) five (b) four (c) three (d) two
ⓐ ⓑ ⓒ ⓓ

(xviii) The number of left (or right) cosets of a subgroup H of a group G is called the _____ of H in G.
(a) order (b) index (c) cardinal (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xix) Let H be a subgroup of a group G, then the number of left cosets is _____ the number of right cosets of H in G.
(a) less than (b) equal to (c) greater than (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xx) If H and K are two finite subgroups of a group G with relatively prime orders, then $H \cap K =$
(a) H (b) K (c) $\{e\}$ (d) none of these
ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.6 Solve / answer the following short questions:

(i) Give an example of an abelian group which is not cyclic. PU, 2012 (BS Math)

(ii) Show that the set of all irrational numbers is not a group under multiplication.

(iii) Show that $ab = ac \Rightarrow b = c$ for any three elements a, b, c of a group G.

(iv) Define a group.

(v) Why the set of all those complex numbers whose module are 1 is not a group under addition?

(vi) Why the set of all irrational numbers is not a group under multiplication.

(vii) Is $(Z, \circ)$ a group? Where $\circ$ is defined by $a \circ b = 0 \; \forall a, b \in Z$.

(viii) Show that the identity element is unique in a group.

(ix) In a group G, show that the inverse of each element is unique.

(x) What is an idempotent?

(xi) If G is a group, then show that $(a^{-1})^{-1} = a \; \forall a \in G$.

(xii) If G is abelian group, then show that $(ab)^2 = a^2b^2 \; \forall a, b \in G$.

(xiii) If each element of a group G is its own inverse, then show that G is an abelian group.

(xiv) If in a group G, $b = xax^{-1}$. Show that $b^2 = xa^2x^{-1}$.

(xv) If in a group G, $b = x^{-1}ax$. Show that $b^2 = x^{-1}a^2x$.

(xvi) If in a group G, $b = x^{-1}a^2x$. Show that $b^2 = x^{-1}a^4x$.

(xvii) If in a group G, $b = xax^{-1}$. Show that $b^3 = xa^3x^{-1}$.

(xviii) If in a group G, $xa = ax$, then show that $xa^2 = a^2x$.

(xix) If in a group G, $xa = ax$, then show that $xa^3 = a^3x$.

(xx) If G is a finite group such that $xy = yz \Rightarrow x = z$ for $x, y, z \in G$, then show that G is abelian.

Q.7 Solve / answer the following short questions:

(i) Let an element a of a group G be of an odd order, then show that there exists an element b in G such that $b^2 = a$.

(ii) Let $(G,*)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $a' = a$, then show that H is a subgroup of G.

(iii) Let $(G,\cdot)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $a^{-1} = a$, then show that H is a subgroup of G.

(iv) Let $(G,+)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $-a = a$, then show that H is a subgroup of G.

(v) Show that every subgroup of an abelian group is abelian.

(vi) Let $(G,\cdot)$ be a group and 'a' be a fixed element of G, show that $H = \{a^k : k \in Z\}$ is a subgroup of G.

(vii) If H is a subgroup of K and K is a subgroup of G, then show that H is a subgroup of G.

(viii) Show that the set of n nth roots of unity is a cyclic group under multiplication.

(ix) Show that every cyclic group is abelian.

(x) If H is a subgroup of a group G, then show that H itself is both left coset and right coset of H in G.

(xi) Define the index of a subgroup.

(xii) Let G be a group of order 89. Can G have a nontrivial subgroup?

(xiii) If each element of a group G is its own inverse, then show that G is an abelian group.

(xiv) Show that the intersection of any collection of subgroups of a group $(G,\cdot)$ is a subgroup of G.

(xv) If H is a subgroup of K and K is a subgroup of G, then show that H is a subgroup of G.

(xvi) Show that every cyclic group is abelian.

(xvii) State Lagrange's theorem.

(xviii) Prove or disprove the set R of real numbers is a group under the operation $\circ$ given by $a \circ b = a + b + 2$.

PU, 2014 (BS Math)

Long Questions

Q.8 Prove that if a and b are elements of a group G and if $a^{-1}b^2a = ba$, then $b = a$.

Q.9 Show that the set $S = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ is a group under multiplication modulo 9. Find order of each element of S.

PU, 2011; 2010 (B.A./B.Sc.)

Q.10 State and prove Lagrange's Theorem.

PU, 2011; 2010 (B.A./B.Sc.)

Q.11 Let H and K be the two finite subgroups of a group G whose orders are relatively prime. Prove that $H \cap K = \{e\}$.

PU, 2003; 2001 (B.A./B.Sc.)

Q.12 Prove that every cyclic group is an abelian group.

PU, 2013; 2012 (BS Math)

Q.13 Let H be a subgroup of a group G and $a \in G$. If $(Ha)^{-1} = \{(ha)^{-1} : h \in H\}$, then show that $(Ha)^{-1} = a^{-1}H$.

PU, 2013; 2012 (B.A./B.Sc.)

Q.14 Let $(G, +)$ be a group. Prove that a nonempty subset K of G is a subgroup of G if and only if $a + (-b) \in K$ for all $a, b \in K$.

PU, 2000 (B.A./B.Sc.)

Q.15 Prove that for all a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$.

PU, 2012 (B.A./B.Sc.)

Q.16 Let G be a group such that $(ab)^n = a^n b^n$ for three consecutive natural numbers n and all $a, b \in G$. Show that G is abelian group.

PU, 2013; 2003; 2002; 2001 (B.A./B.Sc.)

Q.17 Let G be a group and H be a subgroup of G, show that the set $aHa^{-1} = \{aha^{-1} : h \in H, a \in G\}$ is a subgroup of G.

Q.18 Let H be a subgroup of a group G, show that the set of all left cosets of H in G defines a partition of G.

PU, 2003 (B.A./B.Sc.)

Q.19 Let H and K be the subgroups of an abelian group G. Show that the set $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G.

PU, 2002 (B.A./B.Sc.)

Q.20 Show that the union $H \cup K$ of two subgroups H and K of a subgroup G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.

PU, 2002 (B.A./B.Sc.)

PU, 2001 (B.A./B.Sc.)

Q.21 Define an abelian group. If $(G,\cdot)$ is an abelian group, prove that $(xy)^{-1} = x^{-1}y^{-1}$ where $x, y \in G$.

PU, 2000 (B.A./B.Sc.)

Q.22 If H and K are two subgroups of a finite group G, prove that for any $g \in G, g(H \cap K) = gH \cap gK$.

PU, 1999 (B.A./B.Sc.)

Q.23 If G is an abelian group, show $(ab)^n = a^n b^n$ for all $a, b \in G$.

PU, 1999 (B.A./B.Sc.)

Q.24 If G a group and a is a fixed element of G, then show that the subset $H = \{x \in G : ax = xa\}$ of G is a subgroup of G.

PU, 1999 (B.A./B.Sc.)

Q.25 Prove that the order of an element of a finite group divides the order of the group.

PU, 2012 (BS Math)

Q.26 Prove that every subgroup of a cyclic group is cyclic.

PU, 2012 (B.A./B.Sc.); PU, 2012 (BS Math)

Q.27 Show that a finite group whose order is a prime number is necessarily cyclic.

PU, 2012 (BS Math)

Q.28 Show that every left coset is equal to the corresponding right coset in an abelian group.

Q.29 Show that any group of prime order has no non-trivial subgroups.

Q.30 If a is an element of a group G, then show that $a^{|G|} = e$.

Q.31 Let G be an abelian group and H the set of all elements of finite order in G, then show that H is a subgroup of G.

Q.32 Let $(Z,+)$ be a group and H a subset of Z consisting of all the multiples of 5, then show that H is a subgroup of G.

Q.33 Show that the order of a cyclic group is equal to the order of its generator.

Q.34 Show that an infinite cyclic group has exactly two distinct generators.

Q.35 If G is a cyclic group of order n generated by a, then show that for each positive divisor d of n, there is a unique subgroup of G of order d.

SUMMARY

- The nonempty set G is said to be group with respect to $*$ if for all $a,b,c \in G$,
  (i) $a*b \in G$ (ii) $a*(b*c)=(a*b)*c$
  (iii) there exists an element $e \in G$, such that $a*e=e*a=a$.
  (iv) there exists an element $a' \in G$, such that $a*a'=a'*a=e$.
- The group $(G,*)$ is said to be an abelian group or commutative group if $a*b=b*a \ \forall a,b \in G$.
- If G is a nonempty set then the order pair $(G,*)$ is said to be semi group if for all $a,b,c \in G$, (i) $a*b \in G$, (ii) $a*(b*c)=(a*b)*c$.
- In a group G, the identity element is unique.
- In a group G, the inverse of each element is unique.
- An element a of a group G is said to be idempotent if $a^2=a$.
- The only idempotent element in a group is the identity element.
- For any two elements a and b of a group G, the equations $ax=b$ and $ya=b$ have unique solutions.
- If G is a group, then $(a^{-1})^{-1}=a \ \forall a \in G$.
- If G is a group, then $(ab)^{-1}=b^{-1}a^{-1} \ \forall a,b \in G$.
- The number of elements in a group G is called the order of group G and is denoted by $o(G)$ or $|G|$. If the group G consists of finite number of elements then it is said to be a finite group otherwise it is said to be an infinite group.
- If G is a group and $a \in G$, the order or period of 'a' is the least positive integer n such that $a^n=e$.
- If every non-identity element of a group G is of order two, then G is abelian.
- A subset H of a group G is called the subgroup of G if H itself is a group under the same binary operation as defined in G.
- Every group G has at least two subgroups namely G itself and the identity group $\{e\}$. These are called the trivial subgroups of G. Any other subgroup of G is called a non-trivial subgroup of G.
- Let $(G,*)$ be a group. A nonempty subset H of G is a subgroup of G if and only if for all $a,b \in H$, the element $a*b' \in H$, .where b' is the inverse of b.
- Let $(G,\cdot)$ be a group and H be a nonempty finite subset of G such that H is closed under multiplication, then H is a subgroup of G.
- The intersection of any collection of subgroups of a group G is a subgroup of G.

- Union of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.
- Let G be an abelian group and H the set of all elements of finite order in G, then H is a subgroup of G.
- Let $(G,\cdot)$ be an abelian group and H a subset of G consisting of those elements $a \in G$ such that $a^{-1} = a$, then H is a subgroup of G.
- Let G be an abelian group and H a subset of G consisting of those elements of G which are of the second order, then H is a subgroup of G.
- If H, K are subgroups of an abelian group G, then HK is a is a subgroup of G.
- Every subgroup of an abelian group is abelian.
- If H is a subgroup of K and K is a subgroup of G, then show that H is a subgroup of G.
- A group G is said to be cyclic group under multiplication if each element of G is a power of one and the same element of G. Such an element of the group is called the generator of the group.
- The set of n nth roots of unity is a cyclic group under multiplication.
- A group G is said to be a cyclic group under addition generated by 'a' if each element of G is a multiple of 'a'.
- Every cyclic group is abelian.
- $(Q,+)$ is an abelian group but not cyclic.
- Every subgroup of a cyclic group is cyclic.
- The order of a cyclic group is equal to the order of its generator.
- An infinite cyclic group has exactly two distinct generators.
- If G is a cyclic group of order n generated by 'a', then for each positive divisor d of n, there is a unique subgroup of G of order d.
- If G is a cyclic group of even order, then there is only one subgroup of G of order 2.
- If G is a cyclic group of $4n$, where n is a positive integer, then there is only one subgroup of G of order 4.
- If G is a cyclic group of $3n$, where n is a positive integer, then there is only one subgroup of G of order 3.
- Let H be a subgroup of a group G and $a \in G$, then the set $aH = \{ah : h \in H\}$ is said to be the left coset of H in G determined by a.
- Let H be a subgroup of a group G and $a \in G$, then the set $Ha = \{ha : h \in H\}$ is said to be the right coset of H in G determined by a.
- If H is a subgroup of a group G, then H itself is both left coset and right coset of H in G.

- A collection $\{A_\alpha : \alpha \in I\}$ of subsets of a set A is called the partition of A if (i) $A = \bigcup_{\alpha \in I} A_\alpha$ (ii) $A_\alpha \cap A_\beta = \phi$ for $\alpha \neq \beta$.
- Let H be a subgroup of a group G, then the set of all left cosets of H in G defines a partition of G.
- Let H be a subgroup of a group G, then the set of all right cosets of H in G defines a partition of G.
- The number of left (or right) cosets of a subgroup H of a group G is called the *index* of H in G and is denoted by $[G : H]$.
- In an abelian group every left coset is equal to the corresponding right coset.
- Let H be a subgroup of a group G, then the number of left cosets is equal to the number of right cosets of H in G.
- The index and the order of a subgroup of a finite group divide the order of the group.
- The order of an element of a finite group divides the order of the group.
- Any group of prime order is cyclic.
- Any group of prime order has no non-trivial subgroups.
- If a is an element of a group G, then $a^{|G|} = e$.
- If H and K are two finite subgroups of a group G with relatively prime orders, then $H \cap K = \{e\}$.

*****

Chapter

3

GROUPS OF PERMUTATIONS

This chapter is devoted for *Permutation Groups*. These groups are of considerable importance in the quantum mechanics of identical particles. Consider a system of n identical objects. If we interchange any two or more of these objects, the resulting configuration is indistinguishable from the original one. We can consider each interchange as a transformation of the system and then all such possible transformations form a group under which the system is invariant.

In the first section of this chapter we shall define a permutation and then the number of examples will be given to explain the concept of permutations. Finally we shall discuss *even and odd permutations*. Some theorems about even and odd permutations will also be discussed in the last section of this chapter.

3-1 Permutations

In this section first of all we shall study the definition of a permutation with suitable examples, then the inverse permutation will also be defined. The products of permutations will also be discussed in this section.

3-1.1 Definition: Let X be a non-empty set. A bijective mapping $f : X \to X$ is called the *permutation* on X.

If X has n elements, then $n!$ permutations can be taken on X. The permutation f on X is usually written as

$$f = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ f(x_1) & f(x_2) & f(x_3) & f(x_4) & f(x_5) \end{pmatrix},$$

where the first row consists of the elements of X, while the second row consists of their corresponding images under f.

For example, if f is a mapping defined on

$$X = \{1,2,3,4,5,6,7,8\}$$

such that

$$f(1) = 8, \quad f(2) = 1,$$
$$f(3) = 7, \quad f(4) = 4,$$
$$f(5) = 2, \quad f(6) = 5,$$
$$f(7) = 3, \quad f(8) = 6$$

then the permutation f on X is written as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 7 & 4 & 2 & 5 & 3 & 6 \end{pmatrix}$$

Similarly, the permutation α on

$$X = \{x_1, x_2, x_3, x_4, x_5\}$$

defined by

$$\alpha(x_1) = x_4, \quad \alpha(x_2) = x_3, \quad \alpha(x_3) = x_1$$
$$\alpha(x_4) = x_2, \quad \alpha(x_5) = x_5$$

can be written as

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_4 & x_3 & x_1 & x_2 & x_5 \end{pmatrix}.$$

3-1.2 Definition:
Let X be a non-empty set. A permutation $I : X \to X$ is said to be the *identity permutation* on X if

$$I(x) = x \quad \forall x \in X$$

For example,

$$I = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix}$$

is the identity permutation on

$$X = \{x_1, x_2, x_3, x_4, x_5\}$$

Similarly,

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

is the identity permutation on

$$X = \{1,2,3,4,5,6,7,8\}$$

3-1.3 Example: *Find all permutations on* $X = \{1,2,\}$.
Solution: Since X has 2 elements, so there will be $2! = 2$ permutations on X and these permutations are given below:

$$I = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

3-1.4 Example: *Find all permutations on* $X = \{1,2,3\}$.

Solution: Since X has 3 elements, so there will be $3! = 6$ permutations on X and these permutations are given below:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

Interchanging 1 and 2 in I and f_1, we have

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

Interchanging 1 and 3 in I and f_1, we have

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

3-1.5 Example: *Find all permutations on* $X = \{1,2,3,4\}$.

Solution: Since X has 4 elements, so there will be $4! = 24$. Fixing first two columns, we have

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix},$$

Fixing first column and interchanging 2 and 3 in I, f_1

$$f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

Fixing first column and interchanging 2 and 4 in I, f_1

$$f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

Interchanging 1 and 2 in $I, f_1, f_2, f_3, f_4, f_5$, we get

$$f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \qquad f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$f_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \qquad f_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$f_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \qquad f_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

Interchanging 1 and 3 in $I, f_1, f_2, f_3, f_4, f_5$, we get

$$f_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \qquad f_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

$$f_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \qquad f_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix},$$

$$f_{16}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\qquad f_{17}=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},$$

Interchanging 1 and 4 in $I, f_1, f_2, f_3, f_4, f_5$, we get

$$f_{18}=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix},\qquad f_{19}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},$$

$$f_{20}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\qquad f_{21}=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},$$

$$f_{22}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\qquad f_{23}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$

3-1.6 Example:

Find all permutations on $X=\{1,2,3,4,5\}$.[1]

Solution: Since X has 5 elements, so there will be $5!=120$. Fixing first three columns, we have

$$I=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix},\qquad f_1=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$$

Fixing first two columns and interchanging 3 and 4 in I, f_1

$$f_2=\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix},\qquad f_3=\begin{pmatrix}1&2&3&4&5\\1&2&4&5&3\end{pmatrix}$$

Fixing first two columns and interchanging 3 and 5 in I, f_1

$$f_4=\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix},\qquad f_5=\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}$$

Fixing first column and interchanging 2 and 3 in $I, f_1, \ldots, f_5$

$$f_6=\begin{pmatrix}1&2&3&4&5\\1&3&2&4&5\end{pmatrix},\qquad f_7=\begin{pmatrix}1&2&3&4&5\\1&3&2&5&4\end{pmatrix}$$

$$f_8=\begin{pmatrix}1&2&3&4&5\\1&3&4&2&5\end{pmatrix},\qquad f_9=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$$

$$f_{10}=\begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix},\qquad f_{11}=\begin{pmatrix}1&2&3&4&5\\1&3&5&2&4\end{pmatrix}$$

Fixing first column and interchanging 2 and 4 in $I, f_1, \ldots, f_5$

$$f_{12}=\begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix},\qquad f_{13}=\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}$$

[1] The objective of this example is just to assure the students that how 120 permutations are obtained and this is not important for examination point of view.

$$f_{14}=\begin{pmatrix}1&2&3&4&5\\1&4&2&3&5\end{pmatrix},\quad f_{15}=\begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}$$

$$f_{16}=\begin{pmatrix}1&2&3&4&5\\1&4&5&2&3\end{pmatrix},\quad f_{17}=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}$$

Fixing first column and interchanging 2 and 5 in $I, f_1, \ldots, f_5$

$$f_{18}=\begin{pmatrix}1&2&3&4&5\\1&5&3&4&2\end{pmatrix},\quad f_{19}=\begin{pmatrix}1&2&3&4&5\\1&5&3&2&4\end{pmatrix}$$

$$f_{20}=\begin{pmatrix}1&2&3&4&5\\1&5&4&3&2\end{pmatrix},\quad f_{21}=\begin{pmatrix}1&2&3&4&5\\1&5&4&2&3\end{pmatrix}$$

$$f_{22}=\begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix},\quad f_{23}=\begin{pmatrix}1&2&3&4&5\\1&5&2&3&4\end{pmatrix}$$

Interchanging 1 and 2 in $I, f_1, \ldots, f_{23}$, we get

$$f_{24}=\begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix},\quad f_{25}=\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}$$

$$f_{26}=\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix},\quad f_{27}=\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$$

$$f_{28}=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix},\quad f_{29}=\begin{pmatrix}1&2&3&4&5\\2&1&5&3&4\end{pmatrix}$$

$$f_{30}=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix},\quad f_{31}=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$$

$$f_{32}=\begin{pmatrix}1&2&3&4&5\\2&3&4&1&5\end{pmatrix},\quad f_{33}=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$$

$$f_{34}=\begin{pmatrix}1&2&3&4&5\\2&3&5&4&1\end{pmatrix},\quad f_{35}=\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}$$

$$f_{36}=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix},\quad f_{37}=\begin{pmatrix}1&2&3&4&5\\2&4&3&5&1\end{pmatrix}$$

$$f_{38}=\begin{pmatrix}1&2&3&4&5\\2&4&1&3&5\end{pmatrix},\quad f_{39}=\begin{pmatrix}1&2&3&4&5\\2&4&1&5&3\end{pmatrix}$$

$$f_{40}=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix},\quad f_{41}=\begin{pmatrix}1&2&3&4&5\\2&4&5&3&1\end{pmatrix}$$

$$f_{42}=\begin{pmatrix}1&2&3&4&5\\2&5&3&4&1\end{pmatrix},\quad f_{43}=\begin{pmatrix}1&2&3&4&5\\2&5&3&1&4\end{pmatrix}$$

$$f_{44}=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix},\quad f_{45}=\begin{pmatrix}1&2&3&4&5\\2&5&4&1&3\end{pmatrix}$$

$$f_{46}=\begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix},\quad f_{47}=\begin{pmatrix}1&2&3&4&5\\2&5&1&3&4\end{pmatrix}$$

Interchanging 1 and 3 in $I, f_1, \ldots, f_{23}$, we get

$$f_{48}=\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix},\quad f_{49}=\begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}$$

$$f_{50}=\begin{pmatrix}1&2&3&4&5\\3&2&4&1&5\end{pmatrix},\quad f_{51}=\begin{pmatrix}1&2&3&4&5\\3&2&4&5&1\end{pmatrix}$$

$$f_{52}=\begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix},\quad f_{53}=\begin{pmatrix}1&2&3&4&5\\3&2&5&1&4\end{pmatrix}$$

$$f_{54}=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix},\quad f_{55}=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$$

$$f_{56}=\begin{pmatrix}1&2&3&4&5\\3&1&4&2&5\end{pmatrix},\quad f_{57}=\begin{pmatrix}1&2&3&4&5\\3&1&4&5&2\end{pmatrix}$$

$$f_{58}=\begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix},\quad f_{59}=\begin{pmatrix}1&2&3&4&5\\3&1&5&2&4\end{pmatrix}$$

$$f_{60}=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix},\quad f_{61}=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$$

$$f_{62}=\begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix},\quad f_{63}=\begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix}$$

$$f_{64}=\begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix},\quad f_{65}=\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$$

$$f_{66}=\begin{pmatrix}1&2&3&4&5\\3&5&1&4&2\end{pmatrix},\quad f_{67}=\begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix}$$

$$f_{68}=\begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix},\quad f_{69}=\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}$$

$$f_{70}=\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix},\quad f_{71}=\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}$$

Interchanging 1 and 4 in $I, f_1, \ldots, f_{23}$, we get

$$f_{72}=\begin{pmatrix}1&2&3&4&5\\4&2&3&1&5\end{pmatrix},\quad f_{73}=\begin{pmatrix}1&2&3&4&5\\4&2&3&5&1\end{pmatrix}$$

$$f_{74}=\begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix},\quad f_{75}=\begin{pmatrix}1&2&3&4&5\\4&2&1&5&3\end{pmatrix}$$

$$f_{76}=\begin{pmatrix}1&2&3&4&5\\4&2&1&5&3\end{pmatrix},\quad f_{77}=\begin{pmatrix}1&2&3&4&5\\4&2&1&3&4\end{pmatrix}$$

$$f_{78}=\begin{pmatrix}1&2&3&4&5\\4&3&2&1&5\end{pmatrix},\quad f_{79}=\begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$$

$$f_{80}=\begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix},\quad f_{81}=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}$$

$$f_{82}=\begin{pmatrix}1&2&3&4&5\\4&3&5&1&2\end{pmatrix},\quad f_{83}=\begin{pmatrix}1&2&3&4&5\\4&3&5&2&1\end{pmatrix}$$

$$f_{84}=\begin{pmatrix}1&2&3&4&5\\4&1&3&2&5\end{pmatrix},\quad f_{85}=\begin{pmatrix}1&2&3&4&5\\4&1&3&5&2\end{pmatrix}$$

$$f_{86}=\begin{pmatrix}1&2&3&4&5\\4&1&2&3&5\end{pmatrix},\quad f_{87}=\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}$$

$$f_{88}=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix},\quad f_{89}=\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}$$

$$f_{90}=\begin{pmatrix}1&2&3&4&5\\4&5&3&1&2\end{pmatrix},\quad f_{91}=\begin{pmatrix}1&2&3&4&5\\4&5&3&2&1\end{pmatrix}$$

$$f_{92}=\begin{pmatrix}1&2&3&4&5\\4&5&1&3&2\end{pmatrix},\quad f_{93}=\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix}$$

$$f_{94}=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix},\quad f_{95}=\begin{pmatrix}1&2&3&4&5\\4&5&2&3&1\end{pmatrix}$$

Interchanging 1 and 5 in $I, f_1, \ldots, f_{23}$, we get

$$f_{96}=\begin{pmatrix}1&2&3&4&5\\5&2&3&4&1\end{pmatrix},\quad f_{97}=\begin{pmatrix}1&2&3&4&5\\5&2&3&1&4\end{pmatrix}$$

$$f_{98}=\begin{pmatrix}1&2&3&4&5\\5&2&4&3&1\end{pmatrix},\quad f_{99}=\begin{pmatrix}1&2&3&4&5\\5&2&4&1&3\end{pmatrix}$$

$$f_{100}=\begin{pmatrix}1&2&3&4&5\\5&2&1&4&3\end{pmatrix},\quad f_{101}=\begin{pmatrix}1&2&3&4&5\\5&2&1&3&4\end{pmatrix}$$

$$f_{102}=\begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix},\quad f_{103}=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix}$$

$$f_{104}=\begin{pmatrix}1&2&3&4&5\\5&3&4&2&1\end{pmatrix},\quad f_{105}=\begin{pmatrix}1&2&3&4&5\\5&3&4&1&2\end{pmatrix}$$

$$f_{106}=\begin{pmatrix}1&2&3&4&5\\5&3&1&4&2\end{pmatrix},\quad f_{107}=\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}$$

$$f_{108}=\begin{pmatrix}1&2&3&4&5\\5&4&3&2&1\end{pmatrix},\quad f_{109}=\begin{pmatrix}1&2&3&4&5\\5&4&3&1&2\end{pmatrix}$$

$$f_{110}=\begin{pmatrix}1&2&3&4&5\\5&4&2&3&1\end{pmatrix},\quad f_{111}=\begin{pmatrix}1&2&3&4&5\\5&4&2&1&3\end{pmatrix}$$

$$f_{112}=\begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix},\quad f_{113}=\begin{pmatrix}1&2&3&4&5\\5&4&1&3&2\end{pmatrix}$$

$$f_{114}=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix},\quad f_{115}=\begin{pmatrix}1&2&3&4&5\\5&1&3&2&4\end{pmatrix}$$

$$f_{116}=\begin{pmatrix}1&2&3&4&5\\5&1&4&3&2\end{pmatrix},\quad f_{117}=\begin{pmatrix}1&2&3&4&5\\5&1&4&2&3\end{pmatrix}$$

$$f_{118}=\begin{pmatrix}1&2&3&4&5\\5&1&2&4&3\end{pmatrix},\quad f_{119}=\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix}$$

3-1.7 Definition:

Let X be a non-empty set and $f: X \to X$ be a permutation on X such that

$$f(x)=y,\ x,y\in X,$$

then the *inverse permutation*, $f^{-1}: X \to X$ of f is defined as

$$f^{-1}(y)=x,\ x,y\in X$$

Thus

$$f^{-1}=\begin{pmatrix}x_1&x_2&x_3&x_4&x_5\\f^{-1}(x_1)&f^{-1}(x_2)&f^{-1}(x_3)&f^{-1}(x_4)&f^{-1}(x_5)\end{pmatrix}$$

is the inverse permutation of

$$f=\begin{pmatrix}x_1&x_2&x_3&x_4&x_5\\f(x_1)&f(x_2)&f(x_3)&f(x_4)&f(x_5)\end{pmatrix}$$

Similarly,

$$f^{-1}=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&7&4&6&8&3&1\end{pmatrix}$$

is the inverse permutation of

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&7&4&2&5&3&6\end{pmatrix}$$

3-1.8 Example: *Find the inverse permutation of*

$$f=\begin{pmatrix}1&2&3&4&5&6&7\\3&5&4&1&7&2&6\end{pmatrix}$$

Solution: Writing images in the first row and the corresponding pre-images in the second row, we get

$$f^{-1}=\begin{pmatrix}3&5&4&1&7&2&6\\1&2&3&4&5&6&7\end{pmatrix}$$

Rearranging the columns, we get

$$f^{-1}=\begin{pmatrix}1&2&3&4&5&6&7\\4&6&1&3&2&7&5\end{pmatrix}$$

3-1.9 Example: *Find the inverse permutation of*

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\2&3&4&5&6&7&8&9&10&11&12&1\end{pmatrix}$$

Solution: Writing images in the first row and the corresponding pre-images in the second row, we get

$$f^{-1}=\begin{pmatrix}2&3&4&5&6&7&8&9&10&11&12&1\\1&2&3&4&5&6&7&8&9&10&11&12\end{pmatrix}$$

Rearranging the columns, we get

$$f^{-1}=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12\\12&1&2&3&4&5&6&7&8&9&10&11\end{pmatrix}$$

3-1.10 Example: *Find* α^{-1}, β^{-1}, *if*

$$\alpha=\begin{pmatrix}1&2&3&4&5&6\\2&3&6&5&4&1\end{pmatrix},\qquad \beta=\begin{pmatrix}1&2&3&4&5&6\\1&3&5&6&2&4\end{pmatrix}$$

Solution: Interchanging the rows in α, we have

$$\begin{pmatrix}2&3&6&5&4&1\\&&3&4&5&6\end{pmatrix}$$

Rearranging the columns so that the top row reads 1 2 3 4 5 6, we have

$$\alpha^{-1}=\begin{pmatrix}1&2&3&4&5&6\\6&1&2&5&4&3\end{pmatrix}$$

Similarly interchanging the rows in β, we have

$$\begin{pmatrix}1&3&5&6&2&4\\1&2&3&4&5&6\end{pmatrix}$$

Rearranging the columns so that the top row reads 1 2 3 4 5 6, we have

$$\beta^{-1}=\begin{pmatrix}1&2&3&4&5&6\\1&5&2&6&3&4\end{pmatrix}$$

3-1.11 Definition: If $f: X \to X$ and $g: X \to X$ are two permutations on a non-empty set X, then the permutation $fg: X \to X$ on X defined as

$$(x)fg = ((x)f)g \quad \forall x \in X$$

is called the *product or composition of permutations* f and g. It is also denoted by $f \circ g$.

It is clear from the definition that the product of two permutations f and g on $X = \{x_1, x_2, \ldots, x_n\}$ is

$$fg = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ ((x_1)f)g & ((x_2)f)g & \cdots & ((x_n)f)g \end{pmatrix}$$

or

$$fg = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ g(f(x_1)) & g(f(x_2)) & \cdots & g(f(x_n)) \end{pmatrix}$$

In general, $fg \neq gf$.

In permutations, we write the image of x as $(x)f$ in stead of writing $f(x)$. Therefore,

$$f(x) = (x)f$$

3-1.12 Example: *Find the product of following permutations and show that their product does not commute:*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

Solution:

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix}\begin{pmatrix} 5 & 3 & 2 & 6 & 4 & 1 \\ 6 & 1 & 4 & 5 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 5 & 2 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}\begin{pmatrix} 3 & 4 & 1 & 2 & 6 & 5 \\ 2 & 6 & 5 & 3 & 1 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 3 & 1 & 4 \end{pmatrix}$$

$\Rightarrow fg \neq gf$

3-1.13 Example: *Find the product of the permutations:*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

and

$$g=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&2&3&1&6&4&7&5&9\end{pmatrix}$$

Solution:

$$fg=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&2&3&1&6&4&7&5&9\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}2&3&1&4&5&6&7&8&9\\2&3&8&1&6&4&7&5&9\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&8&1&6&4&7&5&9\end{pmatrix}$$

Note: If X consists of the elements $1,2,...,9$, then the symbol $(1,3,4,2,6)$ means the permutation

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&6&4&2&5&1&7&8&9\end{pmatrix}$$

3-1.14 Definition: Two permutations f and g on a nonempty set X are said to be *equal permutations* if

$$(x)f=(x)g \qquad \forall x\in X$$

For example,

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&9&8&7&6&5&4\end{pmatrix}$$

and

$$g=\begin{pmatrix}9&2&3&4&5&8&7&6&1\\4&3&1&9&8&5&6&7&2\end{pmatrix}$$

are equal permutations.

3-1.15 Example:

If $f=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$, *then find* fg, f^2g, f^3g.

Solution:

$$fg=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}2&3&4&1\\1&4&3&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$$

$$f^2=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}2&3&4&1\\3&4&1&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$$

$$\Rightarrow f^2g=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

$$f^3=f^2f=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

$$\Rightarrow f^3g=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$$

3-1.16 Example: *If*

$$f=\begin{pmatrix}1&2&3&4&5&6\\2&4&6&5&3&1\end{pmatrix},\ g=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix},$$

$$h=\begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}$$

Evaluate fg, gf, gh, hg, h^2, g^2.

Solution:

$$fg=\begin{pmatrix}1&2&3&4&5&6\\2&4&6&5&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\2&4&6&5&3&1\end{pmatrix}\begin{pmatrix}2&4&6&5&3&1\\5&1&3&2&4&6\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\5&1&3&2&4&6\end{pmatrix}$$

$$gf=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&4&6&5&3&1\end{pmatrix}$$

$$gf = \begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}6&5&4&1&2&3\\1&3&5&2&4&6\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\1&3&5&2&4&6\end{pmatrix}$$

$$gh = \begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}6&5&4&1&2&3\\3&6&2&5&4&1\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\3&6&2&5&4&1\end{pmatrix}$$

$$hg = \begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}\begin{pmatrix}5&4&1&2&6&3\\2&1&6&5&3&4\end{pmatrix}$$

$$hg = \begin{pmatrix}1&2&3&4&5&6\\2&1&6&5&3&4\end{pmatrix}$$

$$h^2 = hh = \begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\5&4&1&2&6&3\end{pmatrix}\begin{pmatrix}5&4&1&2&6&3\\6&2&5&4&3&1\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\6&2&5&4&3&1\end{pmatrix}$$

$$g^2 = gg = \begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\6&5&4&1&2&3\end{pmatrix}\begin{pmatrix}6&5&4&1&2&3\\3&2&1&6&5&4\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6\\3&2&1&6&5&4\end{pmatrix}$$

3-1.17 Example: *Find $\alpha\beta$, where*

$$\alpha = \begin{pmatrix}2&3&6&7&8&9\\8&6&7&9&2&3\end{pmatrix},\ \beta = \begin{pmatrix}2&3&6&7&8&9\\8&6&7&3&9&2\end{pmatrix}$$

Solution:

$$\alpha\beta = \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 3 & 9 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 2 & 3 \end{pmatrix}\begin{pmatrix} 8 & 6 & 7 & 9 & 2 & 3 \\ 9 & 7 & 3 & 2 & 8 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 & 6 & 7 & 8 & 9 \\ 9 & 7 & 3 & 2 & 8 & 6 \end{pmatrix}$$

3-1.18 Example: *Show that* $f(gh) = (fg)h$, *where*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 3 & 5 & 10 & 7 & 9 & 4 & 2 & 1 & 6 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 6 & 1 & 10 & 2 & 9 & 3 & 4 & 8 \end{pmatrix},$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Solution:

$$gh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 6 & 1 & 10 & 2 & 9 & 3 & 4 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 10 & 1 & 6 & 5 & 7 & 4 & 8 & 9 & 3 \end{pmatrix}$$

$$f(gh) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 3 & 5 & 10 & 7 & 9 & 4 & 2 & 1 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 10 & 1 & 6 & 5 & 7 & 4 & 8 & 9 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 1 & 5 & 3 & 4 & 9 & 6 & 10 & 2 & 7 \end{pmatrix} \quad \ldots(1)$$

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 3 & 5 & 10 & 7 & 9 & 4 & 2 & 1 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 6 & 1 & 10 & 2 & 9 & 3 & 4 & 8 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 10 & 8 & 9 & 4 & 1 & 5 & 7 & 2 \end{pmatrix}$$

$$(fg)h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 10 & 8 & 9 & 4 & 1 & 5 & 7 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 8 & 9 & 10 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 1 & 5 & 3 & 4 & 9 & 6 & 10 & 2 & 7 \end{pmatrix}. \quad \ldots(2)$$

Comparing (1) and (2), we have

$$f(gh) = (fg)h$$

3-2 Cyclic Permutations

In this section we shall discuss a special type of permutations, i.e. *cyclic permutations* or *cycles*. Such permutations have considerable important role in group theory.

3-2.1 Definition:

Let X be nonempty set. Let $Y=\{x_1,x_2,...,x_r\}$ be a subset of X consisting of r elements, then the permutation f on X is said to be *cyclic permutation* or *cycle* of length r if

$$(x_1)f = x_2,$$
$$(x_2)f = x_3,$$
$$(x_3)f = x_4,$$
$$\vdots \quad \vdots$$
$$(x_{r-1})f = x_r,$$
$$(x_r)f = x_1$$

and $$(x)f = x \quad \forall x \in X - Y$$

For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 2 & 3 & 4 & 9 & 6 & 7 & 8 & 11 & 10 & 15 & 12 & 13 & 14 & 1 \end{pmatrix}$$

is a cyclic permutation of length 5. This cyclic permutation is denoted by (1,5,9,11,15). Similarly,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 2 & 4 & 1 & 9 & 6 & 7 & 8 & 11 & 10 & 15 & 12 & 13 & 14 & 3 \end{pmatrix}$$

is a cyclic permutation of length 7. This cyclic permutation is denoted by (1,5,9,11,15,3,4).

3-2.2 Example: *Show that the product of cycles*

$$\alpha = (1,2,5) \quad \textit{and} \quad \beta = (2,1,4,5,6)$$

is not a cycle.

Solution:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 \\ 2 & 5 & 4 & 1 & 6 \end{pmatrix}\begin{pmatrix} 2 & 1 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 2 \end{pmatrix}$$

This example shows that the product of two cycles need not be a cycle.

3-2.3 Definition: If X is a finite set having n elements and f is a permutation on X, then n is called the *degree of permutation f*.

3-2.4 Theorem: *Every permutation of degree n can be written as a product of cyclic permutations acting on mutually disjoint sets.*

PU, 2012 (BS Math); PU, 2010 (B.A./B.Sc.)

Proof: Let f be a permutation of degree n. Let a_1 be one of the elements on which f acts.

Let

$$(a_1)f = a_2$$
$$(a_2)f = a_3$$
$$(a_3)f = a_4$$
$$\vdots \qquad \vdots$$

Since n is finite, there is a natural number k such that

$$(a_k)f = a_1$$

Thus one part of the effect of f is the cyclic permutation

$$f_1 = (a_1, a_2, \ldots, a_k)$$

If $k = n$, then $f = f_1$ is the required cyclic decomposition of f as cyclic permutation. However, if $k < n$, then there are b_i such that

$$(b_1)f = b_2$$
$$(b_2)f = b_3$$
$$\vdots \qquad \vdots$$
$$(b_p)f = b_1$$

Since f is bijective mapping, so these b_i must be different from $a_1, a_2, \ldots, a_k$.

Then one part of f is the cyclic permutation

$$f_2 = (b_1, b_2, \ldots, b_p)$$

Thus we have extracted two cyclic permutations from f.

If $k + p = n$ then f is the product of cycles f_1 and f_2. If, however, $k + p < n$ then the process is continued until a natural number q is obtained such that

$$k + p + \ldots + q = n$$

and one part of the effect of f is a cyclic permutation f_q. Therefore, $f = f_1 f_2 \ldots f_q$, where $f_1, f_2, \ldots, f_q$ act on mutually disjoint subsets of X and uniquely determined. Since any two permutations acting on mutually disjoint sets commute, so apart from the order in which f_i's are taken, $f = f_1 f_2 \ldots f_q$ is unique.

3-2.5 Example: *Express the following permutations as a product of disjoint cycles.*

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 2 & 4 & 1 & 9 & 6 & 7 & 8 & 11 & 10 & 15 & 12 & 13 & 14 & 3 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 9 & 7 & 2 & 4 & 6 & 1 & 11 & 3 & 12 & 8 & 10 \end{pmatrix}$

Solution: (i)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 2 & 4 & 1 & 9 & 6 & 7 & 8 & 11 & 10 & 15 & 12 & 14 & 13 & 3 \end{pmatrix}$$

$$= (1,5,9,11,15,3,4)(13,14)$$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix} = (1,3,4)(2,6)(5,8,7)$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix} = (1,8)(3,6,4)(5,7)$

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 9 & 7 & 2 & 4 & 6 & 1 & 11 & 3 & 12 & 8 & 10 \end{pmatrix}$

$$= (1,5,4,2,9,3,7)(8,11)(10,12)$$

3-3 Order of a Permutation

In this section we shall discuss the order of the permutation with some suitable examples. After discussing the order of a permutation we shall also define the symmetric group.

3-3.1 Definition: The *order of permutation f* on a non-empty set X is the least positive integer n such that $f^n = I$, where I is the identity permutation. For example, the order of

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

is 3, because

$$f^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$
$$= I$$

3-3.2 Theorem:
The order of a cyclic permutation of length n is n.
PU, 2003; 2002 (B.A./B.Sc.)

Proof: Let $f = (a_1, a_2, ..., a_n)$ be a cyclic permutation of length n, then under the action of

$$f : a_1 \to a_2,\ a_2 \to a_3,\ ...,\ a_n \to a_1$$
$$f^2 : a_1 \to a_3,\ a_2 \to a_4,\ ...,\ a_n \to a_2$$
$$f^3 : a_1 \to a_4,\ a_2 \to a_5,\ ...,\ a_n \to a_3$$
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$
$$f^n : a_1 \to a_1,\ a_2 \to a_2,\ ...,\ a_n \to a_n$$

This shows that $f^n = I$. Since n is the least positive integer such that $f^n = I$, so n is the order of f. Hence the cycle of length n has order n.

Note:

To find the order of a permutation f, first decompose f as a product of cyclic permutations

$$f_1, f_2, ..., f_k$$

of lengths $n_1, n_2, ..., n_k$ respectively, ignoring the cycles of length 1 which represent the identity permutation. The order of f is then obtained by taking the least common multiple of $n_1, n_2, ..., n_k$.

3-3.3 Example: *Find the orders of*

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 1 & 7 & 9 & 6 & 5 & 8 & 12 & 11 & 10 \end{pmatrix}$

Solution:

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (1,4,5)(2,3)$

The cycles in the decomposition of f are of lengths 3 and 2. The least common multiple of 3 and 2 is 6, so the order of f is 6.

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = (1,2,3)(4,5,6)$

The cycles in the decomposition of g are of lengths 3 and 3. The least common multiple of 3 and 3 is 3, so the order of g is 3.

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 1 & 7 & 9 & 6 & 5 & 8 & 12 & 11 & 10 \end{pmatrix}$

$= (1,2,3,4)(5,7,6,9,8)(10,12)$

The cycles in the decomposition of h are of lengths 4, 5, and 2. The least common multiple of 4, 5 and 2 is 20, so the order of h is 20.

3-3.4 Theorem: *The set S_n of all permutations on a set X with n elements is a group under the operation of composition of permutations.*

PU, 2011 (B.A./B.Sc.)

Proof: Let X be a nonempty set. Let S_n be a set of all permutations on X, then we have to show that S_n is a group under the operation of composition of permutations.

G_1): Let $f, g \in S_n$, then f and g are bijective mappings on X. Since the composition of two bijective mappings is also a bijective mapping, so $f \circ g$ is a bijective mapping. This shows that $f \circ g \in S_n$. Hence S_n is closed under the operation of composition of permutations.

G_2): The associative law holds in the composition of bijective mappings, so

$$f \circ (g \circ h) = (f \circ g) \circ h \quad \forall f, g, h \in S_n$$

G_3): The identity mapping $I : X \to X$ defined as

$$(x)I = x \qquad \forall x \in X$$

is also a bijective mapping, so I also belongs to S_n.

G_4): The inverse mapping of a bijective mapping is also bijective, so

$$f^{-1} \in S_n \qquad \forall f \in S_n$$

This shows that $(S_n, \circ)$ is a group. Since $f \circ g \neq g \circ f$ in general, so $(S_n, \circ)$ is a non-abelian group.

3-3.5 Definition:

The group $(S_n, \circ)$ of permutations on X is called the *symmetric group* of degree n.

Since each element in S_n is a permutation of n objects (namely elements of X), taken n at a time, there are $n!$ such permutations. Hence the order of S_n is $n!$.

3-3.6 Example: If $X = \{1,2,3\}$, then S_3 consisting of permutations

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$f_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad f_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad f_5=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

is a non-abelian group.

3-3.7 Example:

Find the subgroups of S_3.

Solution:

Since the order of S_3 is 6 and by Lagrange's theorem the order of subgroup of S_3 must divide the order of S_3. The positive divisors of 6 are 1, 2, 3, 6.

The subgroup of order 1 is $H_1=\{I\}$.

The subgroups of order 2 are $\{I,f_3\},\{I,f_4\},\{I,f_5\}$.

The subgroup of order 3 is $H_3=\{I,f_1,f_2\}$.

The subgroup of order 6 is $H_6=S_3=\{I,f_1,f_2,f_3,f_4,f_5\}$.

3-3.8 Example: *Generate the cyclic group by*

$$f=\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}$$

Solution:

$$f^2=\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\5&2&6&4&1&3\end{pmatrix}$$

$$f^3=f^2f=\begin{pmatrix}1&2&3&4&5&6\\5&2&6&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\6&4&1&2&3&5\end{pmatrix}$$

$$f^4=f^3f=\begin{pmatrix}1&2&3&4&5&6\\6&4&1&2&3&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$$

$$=I$$

Thus the cyclic group generated by f is $\{I,f,f^2,f^3\}$.

3-4 Transpositions, Even and Odd Permutations

3-4.1 Definition:

A cycle of length two is called the *transposition*.

The cyclic permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 2 & 9 & 4 & 5 & 6 & 7 & 8 & 3 & 10 & 11 & 12 & 13 \end{pmatrix}$$

is a transposition.

3-4.2 Theorem: *Every cyclic permutation can be expressed as a product of transpositions.*

PU, 2012 (BS Math)

Proof: Let

$$f = (a_1, a_2, a_3, \ldots, a_k) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_2 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix}$$

be a cyclic permutation. Consider the product of transpositions

$$(a_1, a_2)(a_1, a_3)(a_1, a_4)\ldots(a_1, a_k) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_2 & a_1 & a_3 & a_4 & \ldots & a_k \end{pmatrix}$$

$$\times \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_3 & a_2 & a_1 & a_4 & \ldots & a_k \end{pmatrix}$$

$$\times \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_4 & a_2 & a_3 & a_1 & \ldots & a_k \end{pmatrix}$$

$$\vdots$$

$$\times \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_k & a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}$$

$$(a_1, a_2)(a_1, a_3)(a_1, a_4)\ldots(a_1, a_k) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \ldots & a_k \\ a_2 & a_3 & a_4 & a_5 & \ldots & a_1 \end{pmatrix}$$

This shows that

$$(a_1, a_2, a_3, a_4, \ldots, a_k) = (a_1, a_2)(a_1, a_3)(a_1, a_4)\ldots(a_1, a_k)$$

Similarly, we can express the given cyclic permutation as

$$(a_1, a_2, a_3, a_4, \ldots, a_k) = (a_2, a_1)(a_2, a_3)(a_2, a_4)\ldots(a_2, a_k)$$

Hence every cyclic permutation can be expressed as a product of transpositions, possibly in infinitely many ways.

3-4.3 Theorem: *Every permutation of degree n can be expressed as a product of transpositions.*

Proof: Let f be a permutation of degree n, then by theorem 3-2.4 every permutation of degree n can be written as a product of cyclic permutations acting on mutually disjoint sets. Also by theorem 3-4.2,

every cyclic permutation can be expressed as a product of transpositions. Hence f can be expressed as a product of transpositions.

3-4.4 Definition:

A permutation f in S_n is said to be an *even permutation* if it can be written as a product of an even number of transpositions. For example, the number of transpositions in the decomposition of the identity permutation is zero which is an even integers, so the identity permutation is an even permutation.

Similarly, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

is an even transposition, because it can be written as the product of two transpositions, i.e.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4)$$

3-4.5 Example: *Show that the permutation*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

is an even permutation.

Solution:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = (1,3,2,5,4)$$

$$= (1,3)(1,2)(1,5)(1,4)$$

This shows that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

is an even permutation.

3-4.6 Definition:

A permutation f in S_n is said to be an *odd permutation* if it can be written as a product of an odd number of transpositions. Every transposition itself is an odd permutation.

Similarly, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

is an odd permutation, because

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4) = (1,2)(1,3)(1,4)$$

3-4.7 Example: *Show that the permutation*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 7 & 5 \end{pmatrix}$$

is an odd permutation.

PU, 2012; 2001 (B.A./B.Sc.)

Solution:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 7 & 5 \end{pmatrix} = (1,4,2,3)(5,6,7)$$

$$= (1,4)(1,2)(1,3)(5,6)(5,7)$$

Since the given permutation in its decomposition is a product of five transpositions, so it is an odd permutation.

3-4.8 Example: *Show that the permutation*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

is an odd permutation.

Solution:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (1,4,5)(2,3)$$

$$= (1,4)(1,5)(2,3)$$

Since the given permutation in its decomposition is a product of five transpositions, so it is an odd permutation.

3-4.9 Theorem: *The product of two even or odd permutations is an even permutation.*

Proof: Let f and g be any two permutations of degree n, then if f and g can be expressed as a product of m and n transpositions respectively. So the product fg contains $m+n-2k$, where k is a non-negative integer. The term $2k$ occurs because of the possible cancellation of pairs of transpositions.

If both f and g are even permutations, then both m and n will be even and $m+n-2k$ will also be even, so fg will be an even permutation.

3-4.10 Theorem: *The product of an even permutation and an odd permutation is an odd permutation.*

Proof: Let f and g be any two permutations of degree n. Let f be an even permutation and g be an odd permutation, then, the f and g can be expressed as a product of m and n transpositions respectively. So the product fg contains $m+n-2k$, where k is a non-negative integer. The term $2k$ occurs because of the possible cancellation of pairs of transpositions.

Since m is even and n is odd, so $m+n-2k$ is also odd. This shows that fg is an odd permutation.

Since a transposition is an even permutation, so it is clear from above theorems that the product of an even permutation and a transposition is always an odd permutation, because in this case the total number of transpositions becomes an odd number. Similarly, the product of an odd permutation and a transposition is an even permutation. We apply these consequences in proving the following theorem.

3-4.11 Theorem: *The number of even permutations in S_n is equal to the number of odd permutations in S_n for all $n \geq 2$.*

Proof: Let

$$f_1, f_2, \ldots, f_k \quad \ldots(1)$$

be all even permutations and

$$g_1, g_2, \ldots, g_l \quad \ldots(2)$$

all odd permutations in S_n, so that $k+l=n!$

Let h be a transposition, then by previous theorems

$$f_1h, f_2h, \ldots, f_kh \quad \ldots(3)$$

are all odd permutations, while

$$g_1h, g_2h, \ldots, g_lh \quad \ldots(4)$$

are all even permutations. Hence from (2) and (3), we have

$$k \leq l \quad \ldots(5)$$

Similarly, from (1) and (4), we have

$$l \leq k \quad \ldots(6)$$

(5) and (6) $\Rightarrow k=l$.

This completes the proof.

This theorem shows that the number of even permutations and the number of odd permutations in S_n is $\frac{1}{2}(n!)$, because there are total $n!$ number of permutations in S_n.

3-4.12 Theorem: *The set of even permutations is a subgroup of S_3.*

Proof: Let H be the set of all permutations in S_3, then we have to show that H is a subgroup of S_3. For this let $f, g \in H$, then both f and g are even permutations. Since the inverse of an even permutation is also an even permutation, so g^{-1} is an even permutation. Since the product of two even permutations is also an even permutation, so fg^{-1} is an even permutation. Hence $fg^{-1} \in H$. This shows that H is a subgroup of S_3.

Since the product of two odd permutations is an even permutation, so the set of odd permutations is not a subgroup of S_3.

3-4.13 Example: *Write all even and odd permutations in S_3.*

Solution:

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$f_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad f_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad f_5=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

The identity permutation I is an even permutation.

$f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1,2,3)=(1,2)(1,3)$ is an even permutation.

$f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(1,3,2)=(1,3)(1,2)$ is an even permutatio n.

$f_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1,2)$ is an odd permutatio n.

$f_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1,3)$ is an odd permutatio n.

$f_5=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2,3)$ is an odd permutatio n.

EXERCISE 3

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) If X has n elements, then _____ permutations can be taken on X.

(a) n (b) $(n-1)!$ (c) $n!$ (d) $(n+1)!$

ⓐ ⓑ ⓒ ⓓ

(ii) If X has 2 elements, then the number of permutations on X is

(a) 2 (b) 3 (c) 6 (d) 8

ⓐ ⓑ ⓒ ●

(iii) If X has 3 elements, then the number of permutations on X is

(a) 2 (b) 3 (c) 6 (d) 8

ⓐ ⓑ ⓒ ⓓ

(iv) If X has 4 elements, then the number of permutations on X is

(a) 4 (b) 8 (c) 12 (d) 24

ⓐ ⓑ ⓒ ⓓ

(v) If X has 5 elements, then the number of permutations on X is
(a) 5 (b) 10 (c) 24 (d) 120
ⓐ ⓑ ⓒ ⓓ

(vi) The number of permutations on $X = \{1,2,3,4\}$ is
(a) 4 (b) 8 (c) 12 (d) 24
ⓐ ⓑ ⓒ ⓓ

(vii) The identity permutation is
(a) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
(c) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
ⓐ ⓑ ⓒ ⓓ

(viii) If $\alpha = (1,2,3,4)$ is a cyclic permutation of the set $\{1,2,3,4\}$ then $\alpha^2 =$
(a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$
(c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ (d) none of these
ⓐ ⓑ ⓒ ⓓ

(ix) The order of a cyclic permutation of length n is
(a) n (b) $n+1$ (c) $n!$ (d) $(n+1)!$
ⓐ ⓑ ⓒ ⓓ

(x) The group $(S_n, \circ)$ of permutations on X is called the symmetric group of degree
(a) n (b) $n+1$ (c) $n!$ (d) $(n+1)!$
ⓐ ⓑ ⓒ ⓓ

(xi) The order of S_n is
(a) n (b) $n+1$ (c) $n!$ (d) $(n+1)!$
ⓐ ⓑ ⓒ ⓓ

(xii) A cycle of length _____ is called the transposition.
(a) one (b) two (c) three (d) four
ⓐ ⓑ ⓒ ⓓ

(xiii) Every cyclic permutation can be expressed as a _____ of transpositions.
(a) sum (b) difference (c) quotient (d) product
ⓐ ⓑ ⓒ ⓓ

(xiv) The number of even permutations in S_n is _____ the number of odd permutations in S_n for all $n \geq 2$.
(a) less than (b) equal to (c) greater than (d) none
ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.2 Solve / answer the following short questions:

(i) If $f=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, $g=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$, then find $f\circ g$.

(ii) Find $\alpha\beta$, where $\alpha=\begin{pmatrix}2&3&6&7&8&9\\8&6&7&9&2&3\end{pmatrix}$, $\beta=\begin{pmatrix}2&3&6&7&8&9\\8&6&7&3&9&2\end{pmatrix}$.

(iii) Show that the product of cycles $\alpha=(1,2,5)$ and $\beta=(2,1,4,5,6)$ is not a cycle.

(iv) Express $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$ as a product of disjoint cycles.

(v) Express $\begin{pmatrix}1&2&3&4&5&6&7&8\\8&2&6&3&7&4&5&1\end{pmatrix}$ as a product of disjoint cycles.

(vi) If $\alpha=(1,2,3,4)$ is a cyclic permutation of $\{1,2,3,4\}$ then find α^2.

(vii) Show that the permutation $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ is an even transposition.

(viii) Show that the permutation $\begin{pmatrix}1&2&3&4&5&6\\3&5&2&1&6&4\end{pmatrix}$ is an even permutation.

(ix) Show that the permutation $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ is an odd permutation.

Long Questions

Q.3 Prove that every cyclic permutation can be expressed as a product of transpositions.

PU, 2012 (BS Math)

Q.4 Prove that every permutation of degree, n can be written as a product of cyclic permutation acting on mutually disjoint sets.

PU, 2014 (BS Math); PU, 2010 (B.A./B.Sc.)

Q.5 Find the order of the permutation

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$$

PU, 2010 (B.A./B.Sc.)

Q.6 Determine whether the permutation

$$\begin{pmatrix}1&2&3&4&5&6&7\\7&6&5&3&4&2&1\end{pmatrix}$$

is even or odd.

PU, 2011 (B.A./B.Sc.)

Q.7 Show that set S_n of all permutations on a set X with n-elements is a group under the operation of composition of permutations.

PU, 2011 (B.A./B.Sc.)

Q.8 Determine whether the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 2 & 6 & 7 & 5 \end{pmatrix}$$

is even or odd.

PU, 2012; 2001 (B.A./B.Sc.)

Q.9 Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix}$. Find all the elements of cyclic group generated by α.

PU, 2013 (B.A./B.Sc.)

Q.10 Prove that the order of cyclic permutation of length m is m.

PU, 2003; 2002 (B.A./B.Sc.)

Q.11 If $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ is a cyclic permutation, then show that x is not even. Find also n such that $x^n = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

PU, 2000 (B.A./B.Sc.)

SUMMARY

- A bijective mapping $f : X \to X$ is called the permutation on X.
- Every permutation of degree n can be written as a product of cyclic permutations acting on mutually disjoint sets.
- The order of a cyclic permutation of length n is n.
- A cycle of length two is called the transposition.
- Every cyclic permutation can be expressed as a product of transpositions.
- Every permutation of degree n can be expressed as a product of transpositions.
- A permutation f in S_n is said to be an even permutation if it can be written as a product of an even number of transpositions.
- A permutation f in S_n is said to be an odd permutation if it can be written as a product of an odd number of transpositions.
- The product of two even or odd permutations is an even permutation.
- The product of an even permutation and an odd permutation is an odd permutation.

*****

Chapter

4

GROUPS OF SYMMETRIES

In this chapter, we shall be concerned with very important and special types of groups which arise from the symmetries of shapes. Such groups play vital role in chemistry, specially, in molecular structures and chemical bonds.

4-1 Types of Symmetries

In this section first we define symmetry and then we discuss some different types of symmetries.

What is Symmetry?

Symmetry is perhaps most familiar as an artistic or aesthetic concept. Designs are said to be symmetric if they exhibit specific kinds of balance, repetition, and/or harmony.

In mathematics, symmetry is more akin to something like "constancy," or how something can be manipulated without changing its form. In other words, the mathematical notion of symmetry relates to "objects" that appear unchanged when certain transformations are applied.

4-1.1 Mirror Symmetry:

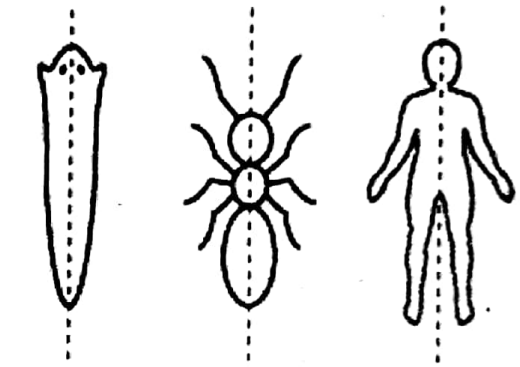
When we say that something is symmetric we are usually thinking of left-right symmetry.

For example, a design is symmetric in this way if the right half is the mirror image of the left. The *axis of symmetry* separates the two halves and, if we place a mirror along this line, the design seems complete. The reflection of the left half makes up for the hidden right half.

Think of the form of a butterfly; its right and left halves mirror each other. If you knew what the right half of a butterfly looked like, you could construct the left half by reflecting the right half over a line that bisects the butterfly.

Axis of Reflection Symmetry Axis of Reflection Symmetry

The axis of reflection symmetry of Flatworm, Ant and Human are shown below:

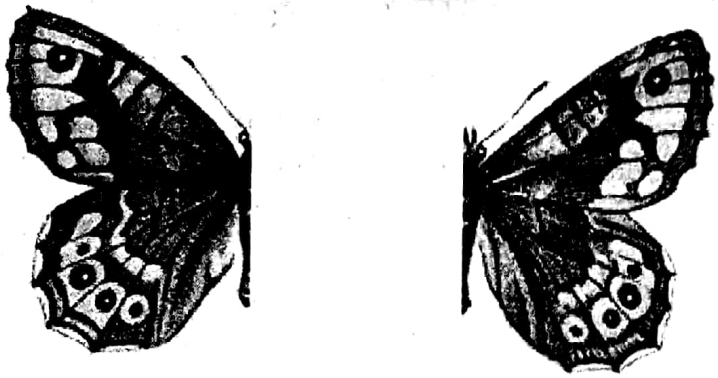


Flatworm Ant Human

Butterflies exhibit a type of symmetry called *bilateral symmetry* or a *mirror symmetry*, (either half of the butterfly is the mirror image of the other) one that is very common among living things. Perhaps most familiar to us is our own bilateral symmetry, the symmetry of our left and right arms and hands, or our left and right legs and feet, or the approximate symmetry of our bodies if bisected vertically into left and right halves.

In general, bilateral symmetry is present whenever an object or design can be broken down into two parts, one of which is the reflection of the other. In the following the butterfly

is broken down into two parts, one of which is the reflection of the other.



Given any motif, one can generate a design with bilateral symmetry by choosing a line and reflecting the motif over it. Conversely, if a motif already possesses bilateral symmetry, it can be reflected over a line and we would notice no difference between the original and the reflected versions. This action, reflection, leaves the original design apparently unchanged, or *invariant*.

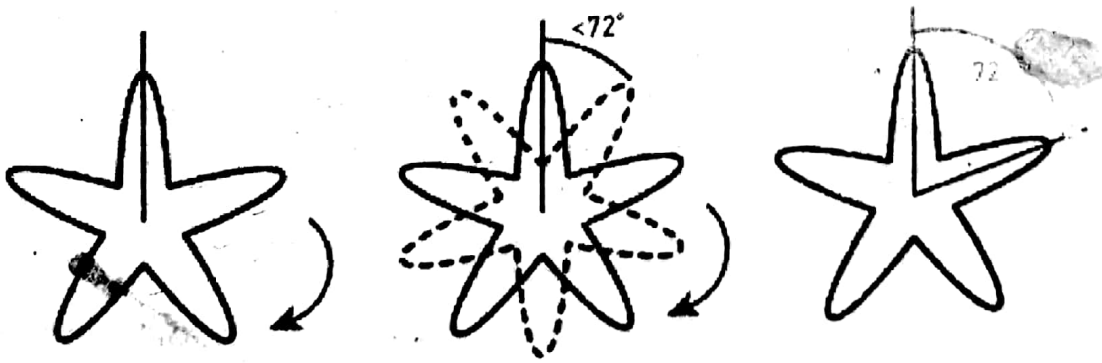
Bilateral symmetry is quite common in nature, but it is by no means the only form of visual symmetry that we see in the world around us. Another common form is *rotational symmetry*, such as that seen in sea stars and daisies.

4-1.2 Rotational Symmetry:

Recall that to be symmetric an object must appear unchanged after some action has been taken on it. An object that exhibits *rotational symmetry* will appear unchanged if it is rotated through some angle.

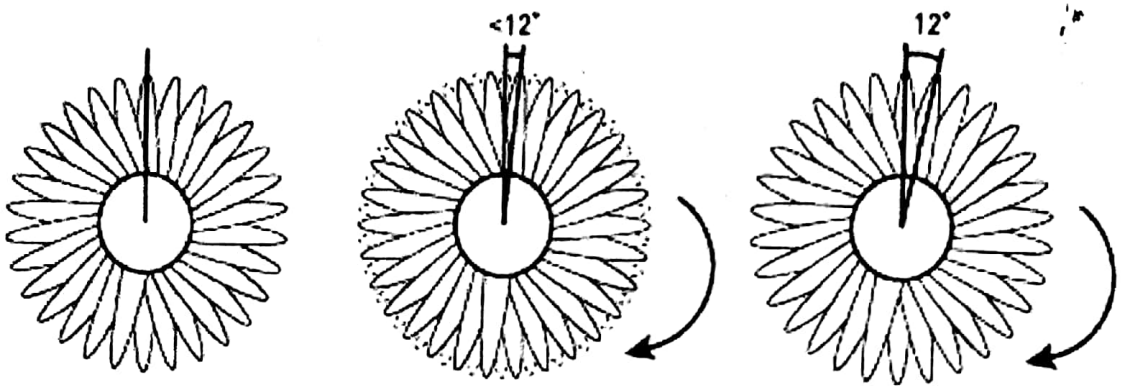
A circle can be rotated any amount and still look like a circle, but most objects can be rotated only by some specific amount, depending on the exact design.

For example, an ideal sea star, having five arms, is not symmetric under all rotations, but only those equivalent to $\frac{1}{5}$ of a full rotation, i.e. $\frac{1}{5}(360°)$ or 72°.



Rotating an ideal sea star 72° leaves its appearance unchanged.

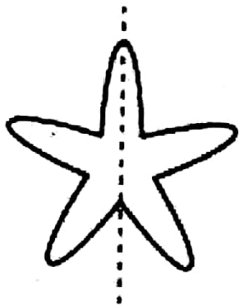
A daisy, on the other hand, is rotationally symmetric under smaller rotational increments. Let us say it has 30 petals, all of which are the same in appearance— no such daisy exists in the real world, of course— this is an ideal mathematical daisy. The flower will be symmetric under a rotation of $\frac{1}{30}$ of a full rotation, i.e. $\frac{1}{30}(360°)$ or 12° or any multiple thereof.



The ideal daisy is symmetric under rotations of 12°

We might have observed that the sea star and the daisy are not limited to rotational symmetry. Depending on how you choose an axis of reflection, they can each display bilateral (reflection) symmetries as well.

Notice, however, that only certain dividing lines can serve as axes of reflection.



Axis of Reflection Symmetry

Not an Axis of Reflection Symmetry

This brings us to an important point: an object may have more than one type of symmetry. The specific symmetries that an object exhibits help to characterize its shape. Remember, the motions associated with symmetries always leave the object invariant. This means that combinations of these motions, which are how mathematicians tend to think of symmetries, will also leave the original object invariant.

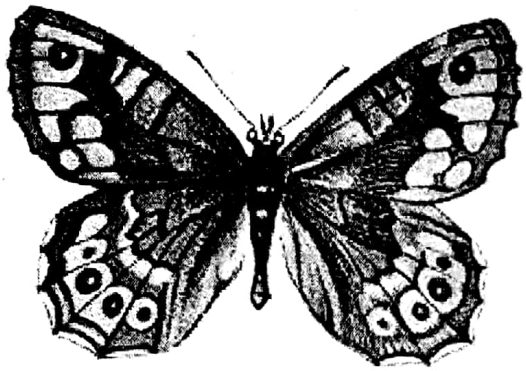
4-1.3 Order of Rotational Symmetry:

The number of rotations required for all the points to actually return to their original positions is called the *order* or *degree of the rotation*.

For example, the order of the rotation of an ideal sea star is 5. In other words, we say that an ideal sea star has 5-fold symmetry.

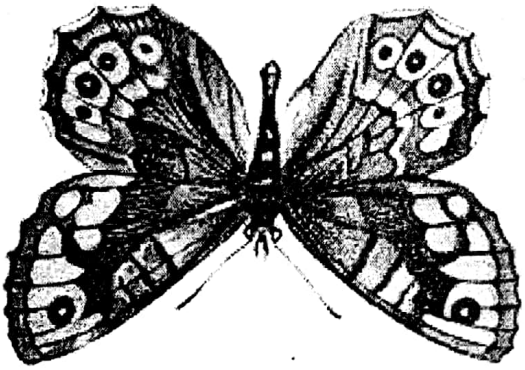
Similarly, the order of the rotation of above mentioned daisy is 30, i.e. daisy has 30-fold symmetry.

In the following we show the counter clockwise rotations of butterfly:



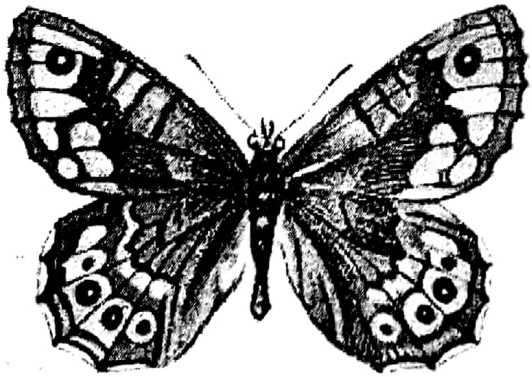
Initial Position

First Rotation of 90°



Second Rotation of 90°

Third Rotation of 90°



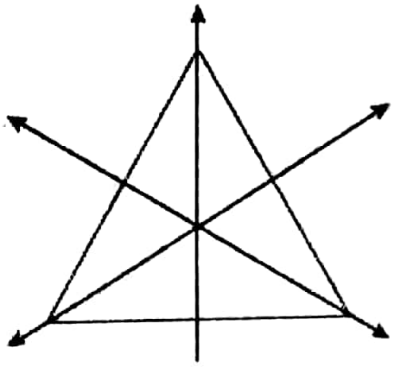
Fourth Rotation of 90° = Initial Position

This shows that the butterfly has a rotational symmetry of order 4 or 4-fold symmetry.

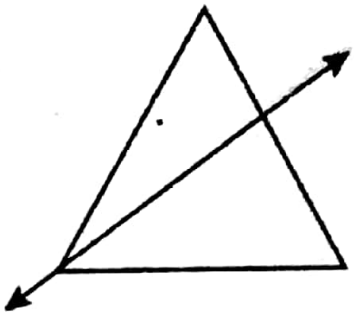
4-1.4 Example: *Find the axes of reflection symmetry of an equilateral triangle and show that it has 3-fold symmetry.*

Solution: The rotational symmetries of the equilateral triangle can be thought of as the rotations that leave the triangle invariant.

In the following, we see that there are three lines over which the triangle can be reflected and maintain its original appearance, so an equilateral triangle has three axes of reflectional symmetry.



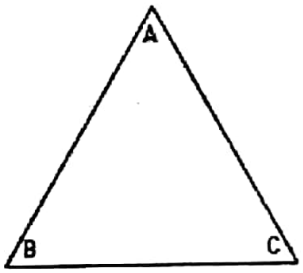
Three Axes of
Reflection Symmetry



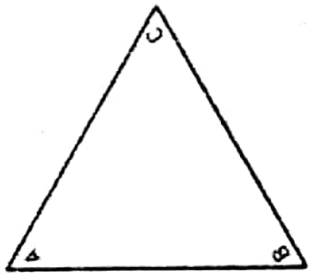
Not an Axis of
Reflection Symmetry

An equilateral triangle is symmetric under those rotations which are equivalent to $\frac{1}{3}$ of a full rotation, i.e. $\frac{1}{3}(360°)$ or 120°.

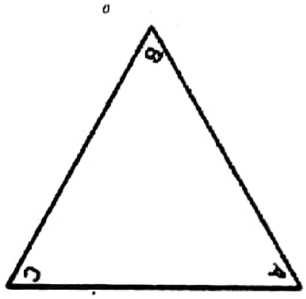
In the following we show the counter clockwise rotations of equilateral triangle *ABC*.



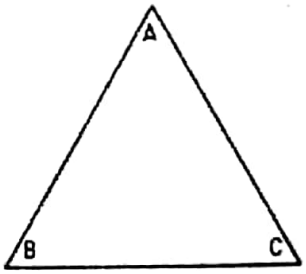
Initial Position



First Rotation of 120°



Second Rotation of 120°



Third Rotation of 120° = Initial Position

This shows that the equilateral triangle has a rotational symmetry of order 3 or 3-fold symmetry.

4-2 The Symmetry Group of an Equilateral Triangle

After detailed discussion of reflection and rotational symmetries, we are in a position to present groups of symmetries. In this section, we shall show how the reflection and rotational symmetries of an equilateral triangle form a group.

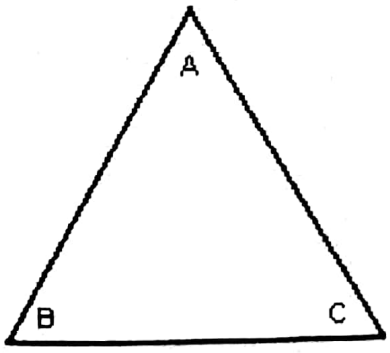
4-2.1 Symmetry Group of Equilateral Triangle/ Dihedral Group D_6:

There are six motions that can bring an equilateral triangle back into its original position. They are

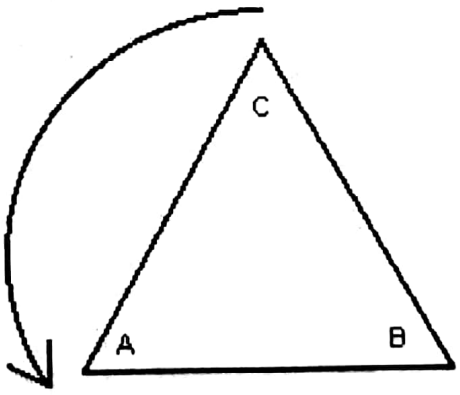
- Do nothing
- Rotate 120 degrees counter clockwise
- Rotate 240 degrees counter clockwise
- Flip about the symmetry axis through the upper vertex
- Flip about the symmetry axis through the lower left-hand vertex
- Flip about the symmetry axis through the lower right-hand vertex

There are other motions but they are "equivalent" to those listed above. For example rotating the triangle 360 degrees is "equivalent" to doing nothing since the basic orientation of the triangle is unchanged.

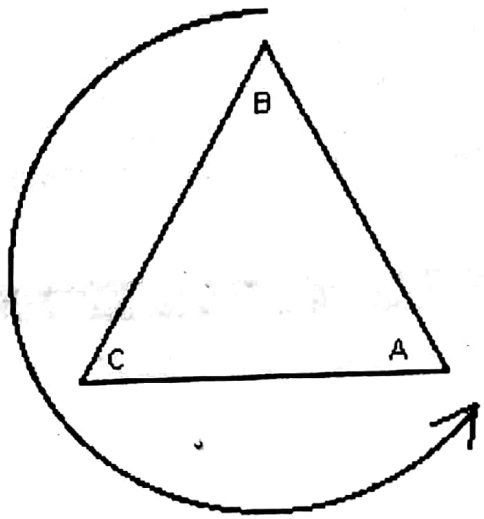
We have labelled the vertices *A*, *B* and *C* and have shown the 6 symmetry motions below:



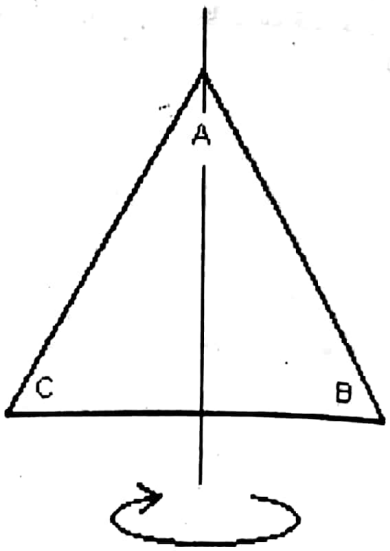
The equilateral triangle before a movement and after any movement that does not change anything (like rotating it 360 degrees).



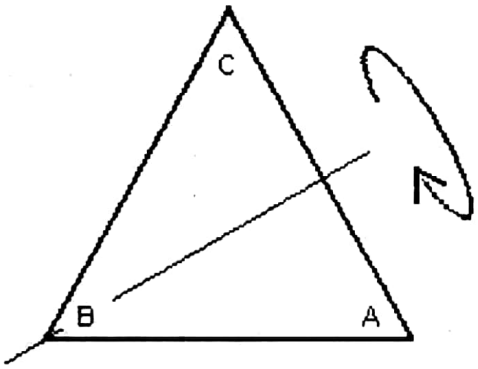
The equilateral Triangle after being rotated 120 degrees counter clockwise.



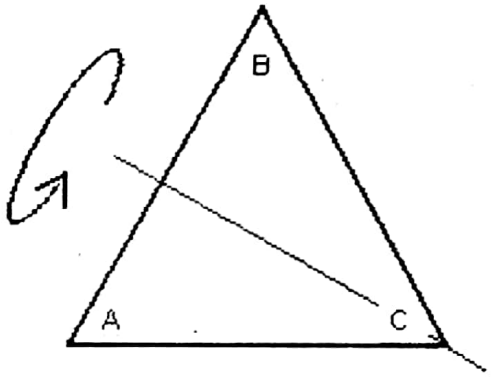
The triangle after being rotated 240 degrees counter clockwise.



The Triangle after being flipped about the axis through the upper vertex.



The triangle after being flipped about the axis through the lower left-hand vertex.



The triangle after being flipped about the axis through the lower right-hand vertex.

Now we are in a position to combine these symmetry operations of the triangle to form a group. We simply use the operation of **followed by** and find that

- **We have closure:** performing one motion *followed by* performing another motion is equivalent (has the same effect) as performing one of the 6 motions.
- **We have associativity:** since *followed by* is always an associative operation.
- **We have an identity:** The **Do nothing** motion is the identity element.
- **We have Inverses:** Each element has an inverse:
  - The **Do nothing** is its own inverse.
  - The **Rotate 120 degrees** and the **Rotate 240 degrees** are inverses of each other.
  - The three **Flip** movements are their own inverses.

It is advised that one should make a paper or cardboard triangle and label its vertices ***A***, ***B*** and ***C***. Then draw a similar triangle on a piece of paper. Begin with the triangle in the start position (as shown in the first illustration) and perform the various motions, one after another. Note the final orientation of the triangle (by the distribution of its vertices) after the two motions have been performed (one *followed by* another). What single motion is this equivalent to?

Continuing this way we can fill in a Cayley table for the **Symmetry Group of the Equilateral Triangle**.
So, let us do it. We shall need some symbols to stand for our movements.

If we denote the original position of equilateral triangle *ABC* by *e*, then there are two counter clockwise rotations of 120° of the triangle before it comes to its original position *e*, so it is suggested that these two rotations should be denoted by *a* and a^2 respectively.

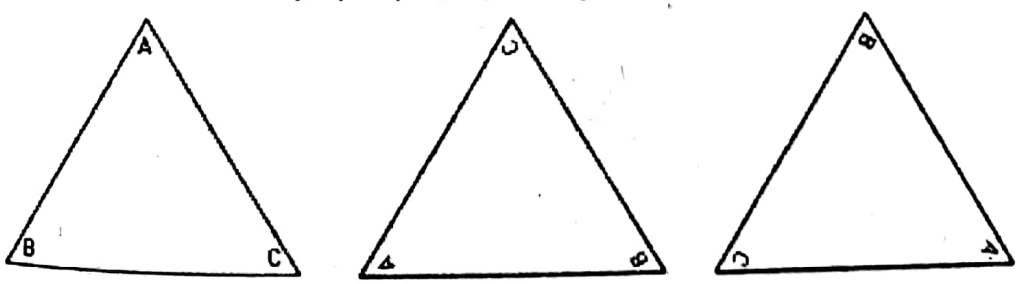
For a flip about the axis of reflection symmetry through the vertex *A*, it is suggested to denote this flip by *b*.

Similarly, the flips about the axes of reflection symmetry through the vertices *B* and *C* are suggested to denote by *x* and *y* respectively.

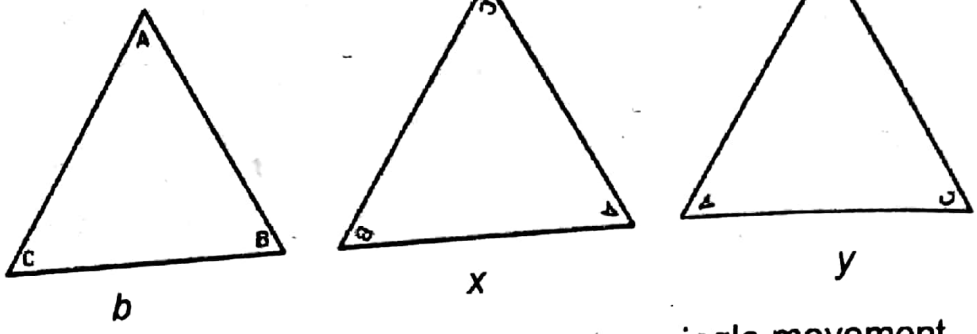
So let us assume

- ***e*** stands for the **Do nothing** movement.
- ***a*** stands for the **Rotate 120** degrees counter clockwise movement.
- a^2 stands for the **Rotate 240** degrees counter clockwise movement.
- ***b*** stands for the **Flip** about axis through the top vertex ***A*** movement.
- ***x*** stands for the **Flip** about the axis through the lower-left vertex ***B*** movement.
- ***y*** stands for the **Flip** about the axis through the lower-right vertex ***C*** movement.

In order to complete Cayley table, first we write the following triangles using the definitions of ***e***, ***a***, a^2, ***b***, ***x***, and ***y***:



e ***a*** a^2



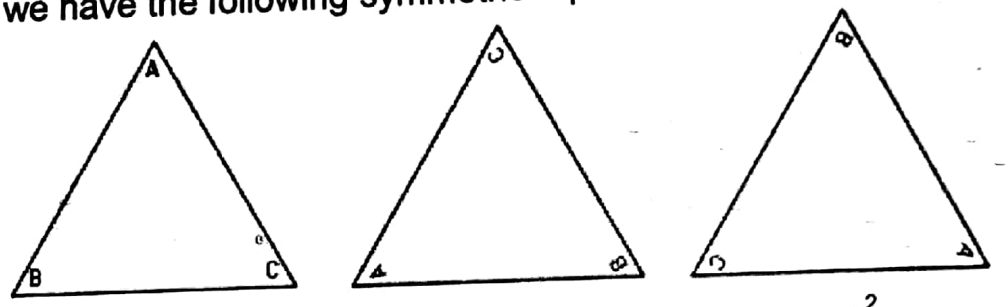
b *x* *y*

Each of the above six triangles represents a single movement.
It is clear that if we rotate triangle *b* counter clock wise through 240°, we obtain triangle *x*, i.e.

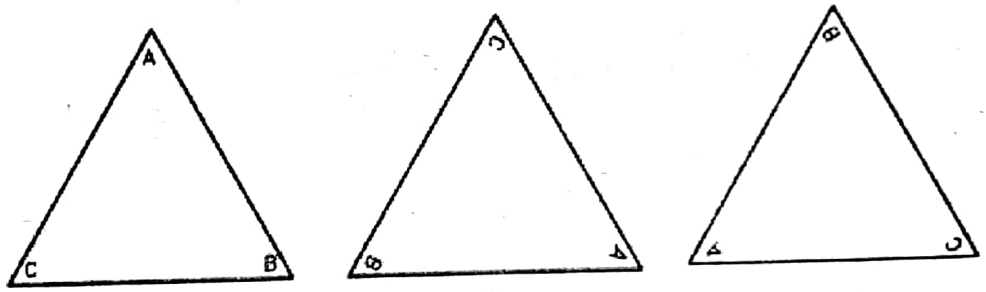
$$x = a^2b$$

Similarly, if we rotate triangle *b* counter clock wise through 120°, we obtain triangle *y*, i.e. $y = ab$

Thus, we have the following symmetric equilateral triangles:



e *a* a^2



b a^2b ab

In order to make Cayley table, first we write elements

$$e, a, a^2, b, ab, a^2b$$

in the first row and the first column as follws:

•	e	a	a^2	b	ab	a^2b
e						
a						
a^2						
b						
ab						
a^2b						

Table-1

In the following, we discuss some of the multi movements.

- $e \cdot e$ stands for the **Do nothing** movement to triangle e, so $e \cdot e = e$.
- $e \cdot a$ stands for the **Do nothing** movement to triangle a, so $e \cdot a = a$.
- Similarly, $e \cdot b = b$, $e \cdot x = x$, $e \cdot y = y$, $e \cdot z = z$, $a \cdot e = a$, $b \cdot e = b$, $x \cdot e = x$, $y \cdot e = y$, $z \cdot e = z$.
- $a \cdot a$ stands for the **Rotate 120** degrees counter clockwise movement the triangle a. This gives us triangle a^2, so $a \cdot a = a^2$.
- $a \cdot a^2$ stands for the **Rotate 120** degrees counter clockwise movement the triangle a^2. This gives us triangle e, so $a \cdot a^2 = e$.
- $a^2 \cdot a$ stands for the **Rotate 240** degrees counter clockwise movement the triangle e. This gives us triangle e, so $a^2 \cdot a = e$.
- $a^2 \cdot a^2$ stands for the **Rotate 240** degrees counter clockwise movement the triangle a^2. This gives us triangle a, so $a^2 \cdot a^2 = a$.
- $a^2 \cdot ab$ stands for the **Rotate 240** degrees counter clockwise movement the triangle ab. This gives us triangle b, so $a^2 \cdot ab = b$.
- $ab \cdot a^2$ stands for the **Flip** about the axis through the lower-right vertex **C** movement the triangle ab. This gives us triangle a^2b, so $ab \cdot a^2 = a^2b$.

Continuing in this way, we complete the Cayley table (Table-1) as follows:

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Table-2: Cayley table of symmetry group of equilateral triangle

The symmetr group of an equal triangle is also known as *dihedral group* D_6 Thus the dihedral group D_6 is

$$D_6 = \{ e, a, a^2, b, ab, a^2b \}$$

It is also denoted by S_3 and is written as

$$S_3 = \{ e, a, a^2, b, ab, a^2b \}$$

In the following we give another way of writing S_3 group:

$$S_3 = < a, b : a^3 = b^2 = (ab)^2 = e >$$

4-2.2 Example: *Find all subgroups of dihedral group D_6.*

Solution: The dihedral group D_6 is given below:

$$D_6 = \{ e, a, a^2, b, ab, a^2b \}$$

It consists of 6 elements, so by Lagrange's theorem, orders of subgroups must divide 6 (the order of D_6).

The positive divisors of 6 are

$$1, 2, 3, 6.$$

Therefore, the subgroups of D_6 must be of orders

$$1, 2, 3, 6$$

Subgroup of order 1 is the identity element group, i.e.

$$\{ e \}$$

Subgroup of order 6 is the D_6 group itself, i.e.

$$\{ e, a, a^2, b, ab, a^2b \}$$

Subgroup of order 3 is the rotational subgroup

$$\{ e, a, a^2 \}$$

It is clear that a is obtained by rotating e counter clockwise through 120°. a^2 is obtained by rotating a counter clockwise through 120°. Finally, rotating a^2 counter clockwise through 120°, we get e.

Subgroups of order 2 are the flip subgroups

$$\{ e, b \}, \{ e, ab \}, \{ e, a^2b \}$$

For the subgroup

$$\{ e, b \}$$

it is clear that b is obtained by flipping e about axis through the top vertex A.

For the subgroup

$$\{ e, ab \}$$

it is clear that ab is obtained by flipping e about axis through the vertex B.

For the subgroup

$$\{ e, a^2b \}$$

it is clear that ab is obtained by flipping e about axis through the vertex C.

Note:

There are following four proper subgroups of dihedral group D_6:

Rotational subgroup: $\{ e, a, a^2 \}$

Flip subgroups: $\{ e, b \}, \{ e, ab \}, \{ e, a^2b \}$

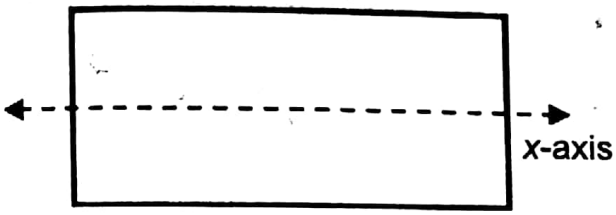
4-3 The Symmetry Group of a Rectangle

In this section, first we find the axes of symmetry of a rectangle, then we shall find the symmetry group of rectangle.

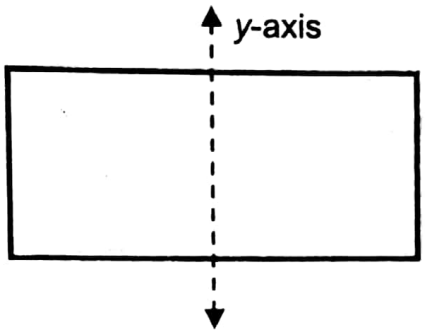
4-3.1 Example: *Find the axes of reflection symmetry of a rectangle and show that it has 2-fold symmetry.*

Solution: The rotational symmetries of the rectangle can be thought of as the rotations that leave the rectangle invariant.

In the following, we see that there are two lines over which the rectangle can be reflected and maintain its original appearance, so a rectangle has two axes of reflection symmetry.



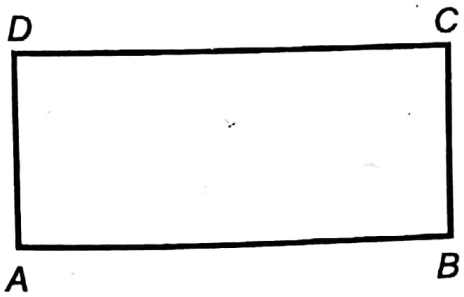
Axis of Reflection Symmetry



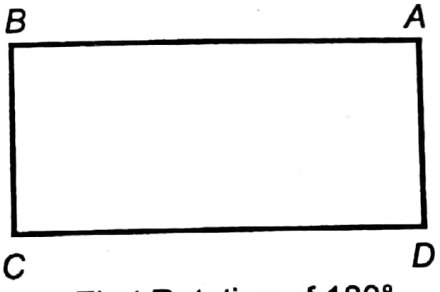
Axis of Reflection Symmetry

A rectangle is symmetric under those rotations which are equivalent to $\frac{1}{2}$ of a full rotation, i.e. $\frac{1}{2}(360°)$ or 180°.

In the following we show the counter clockwise rotations of rectangle *ABCD*.



Initial Position



First Rotation of 180°

Second Rotation of 180° = Initial Position

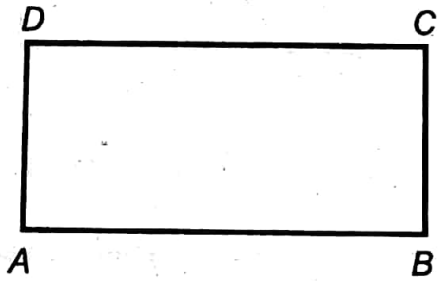
This shows that the rectangle has a rotational symmetry of order 2 or 2-fold symmetry.

The Symmetry Group of the Rectangle/ Klein 4-Group:

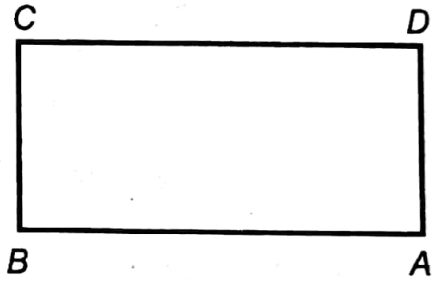
There are four motions that can bring a rectangle back into its original position. They are

- Do nothing
- Flip about the symmetry axis (y-axis)
- Flip about the symmetry axis (x-axis)
- Rotate 180 degrees counter clockwise

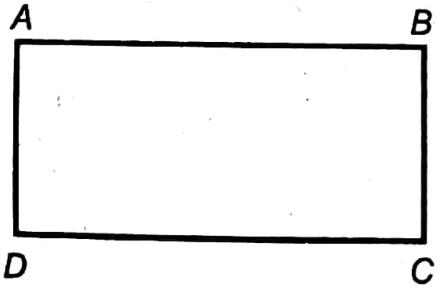
We have labelled the vertices A, B, C and D and have shown the 4 symmetry motions below:



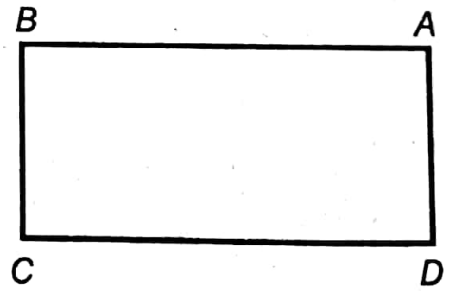
Initial Position



Flip about y-axis



Flip about x-axis

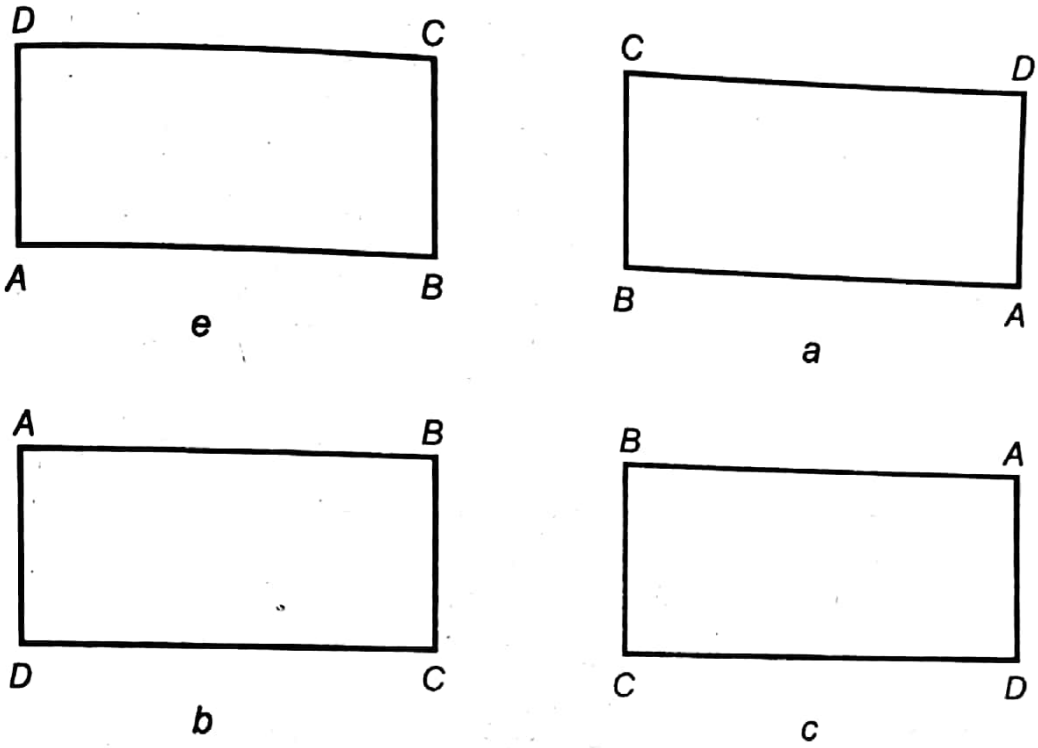


Rotation of 180°

We shall need some symbols to stand for our movements. So let us assume

- **e** stands for the **Do nothing** movement.
- ***a*** stands for the **Flip** about ***y*-axis**.
- ***b*** stands for the **Flip** about ***x*-axis**.
- ***c*** stands for the **Rotate 180°** counter clockwise movement.

In order to complete Cayley table, first we write the following rectangles using the definitions of **e, a, b,** and **c**:



Note that each *a* and *b* rectangle represents a single movement while rectangle *c* is a multi movement. Because, if we flip rectangle *a* about *x*-axis, we get rectangle *c*, so $c = ab$.

It is also clear that the flip of *a* about *y*-axis gives *e*, i.e. $a^2 = e$.

Similarly, the flip of *b* about *x*-axis gives *e*, i.e. $b^2 = e$.

The rotation of *c* about *x*-axis gives *e*, i.e. $c^2 = e$, i.e. $(ab)^2 = e$.

We conclude that:

- **We have closure:** performing one motion *followed by* performing another motion is equivalent (has the same effect) as performing one of the 4 motions.
- **We have associativity:** since *followed by* is always an associative operation.
- **We have an identity:** The **Do nothing** motion is the identity element.
- **We have Inverses:** Each element has an inverse:
    - The **Do nothing** is its own inverse.
    - The two **Flip** movements are their own inverses, since $a^2 = e$, $b^2 = e$, so $a^{-1} = a$, $b^{-1} = b$.
    - The **Rotate 180°** is its own inverse, since $(ab)^2 = e$, so $(ab)^{-1} = ab$.

The corresponding Cayley table is given below:

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Table-3: Cayley table of symmetry group of rectangle

The symmetry group of a rectangle is also known as *Klein 4-group* V_4. Thus the Klein 4-group V_4 is

$$V_4 = \{ e, a, b, ab \}$$

In the following we give another way of writing V_4 group:

$$V_4 = < a, b : a^2 = b^2 = (ab)^2 = e >$$

4-3.2 Example: *Find all subgroups of Klein 4-group* V_4.

Solution: The Klein 4-group V_4 is given below:

$$V_4 = \{ e, a, b, ab \}$$

It consists of 4 elements, so by Lagrange's theorem, orders of subgroups must divide 4 (the order of V_4). The positive divisors of 1 are 1, 2, 4. Therefore, the subgroups of V_4 must be of orders 1, 2, 4.

Subgroup of order 1 is the identity element group, i.e.

$$\{ e \}$$

Subgroup of order 4 is the V_4 group itself, i.e.

$$\{ e, a, b, ab \}$$

Subgroups of order 2 are the flip subgroups

$$\{ e, a \}, \{ e, b \}$$

and the rotational subgroup

$$\{ e, ab \}$$

For the subgroup

$$\{ e, a \}$$

it is clear that a is obtained by flipping e about y-axis.

For the subgroup

$$\{ e, b \}$$

it is clear that b is obtained by flipping e about x-axis.

For the subgroup

$$\{ e, ab \}$$

it is clear that ab is obtained by rotating e counter clockwise through 180°.

Note: There are following three proper subgroups of Klein 4-group V_4:

Flip subgroups: $\{ e, a \}, \{ e, b \}$

Rotational subgroup: $\{ e, ab \}$

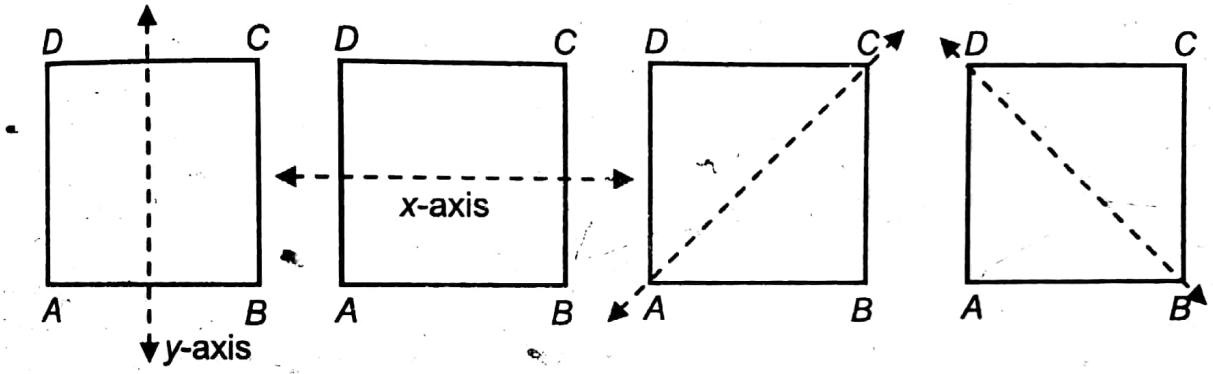
4-4 The Symmetry Group of a Square

In this section, first we find the axes of symmetry of a square, then we shall find the symmetry group of square.

4-4.1 Example: *Find the axes of reflection symmetry of a square and show that it has 4-fold symmetry.*

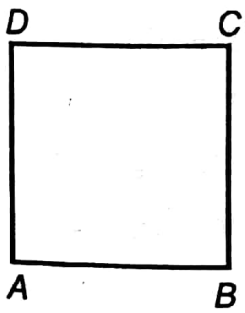
Solution: The rotational symmetries of the square can be thought of as the rotations that leave the square invariant.

In the following, we see that there are four lines over which the square can be reflected and maintain its original appearance, so a square has four axes of reflection symmetry.

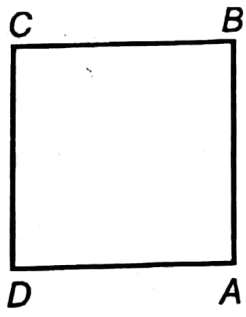


A square is symmetric under those rotations which are equivalent to $\frac{1}{4}$ of a full rotation, i.e. $\frac{1}{4}(360°)$ or 90°.

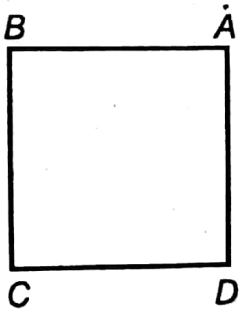
In the following we show the counter clockwise rotations of square *ABCD*.



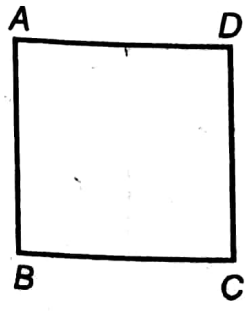
Initial Position



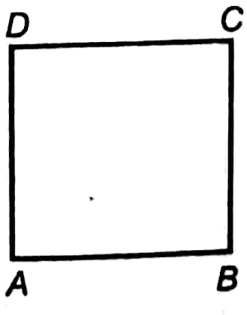
First Rotation of 90°



Second Rotation of 90°



Third Rotation of 90°



Fourth Rotation of 90° = Initial Position

This shows that the square has a rotational symmetry of order 4 or 4-fold symmetry.

The Symmetry Group of the Square/ Dihedral Group D_4:

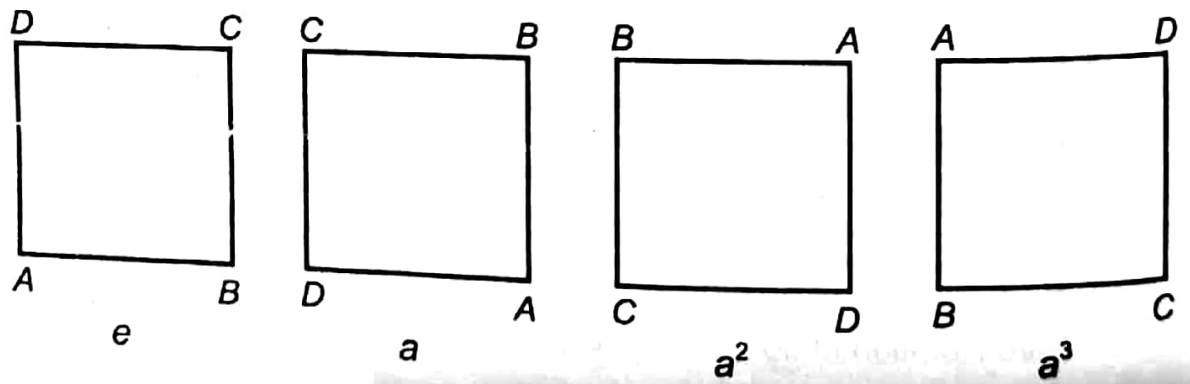
There are eight motions that can bring a square back into its original position. They are

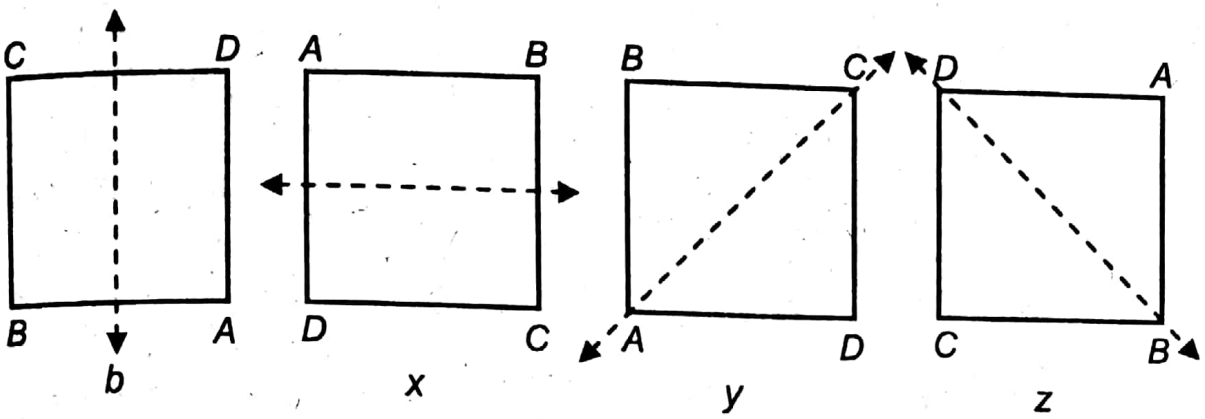
- Do nothing
- Rotate counter clockwise through 90°
- Rotate counter clockwise through 180°
- Rotate counter clockwise through 270°
- Flip about the symmetry axis (y-axis)
- Flip about the symmetry axis (x-axis)
- Flip about the symmetry axis (through AC)
- Flip about the symmetry axis (through BD)

We use the following symbols to stand for our movements.

- ***e*** stands for the **Do nothing** movement.
- ***a*** stands for **Rotate** counter clockwise through **90°**.
- $\boldsymbol{a^2}$ stands for **Rotate** counter clockwise through **180°**.
- $\boldsymbol{a^3}$ stands for **Rotate** counter clockwise through **270°**.
- ***b*** stands for **Flip** about the symmetry axis **(*y*-axis)**.
- ***x*** stands for **Flip** about the symmetry axis **(*x*-axis)**.
- ***y*** stands for **Flip** about the symmetry axis **(through *AC*)**.
- ***z*** stands for **Flip** about the symmetry axis **(through *BD*)**.

In order to complete Cayley table, first we write the following squares using the definitions of **e**, ***a***, $\boldsymbol{a^2}$, $\boldsymbol{a^3}$, ***b***, ***x***, ***y*** and ***z***:





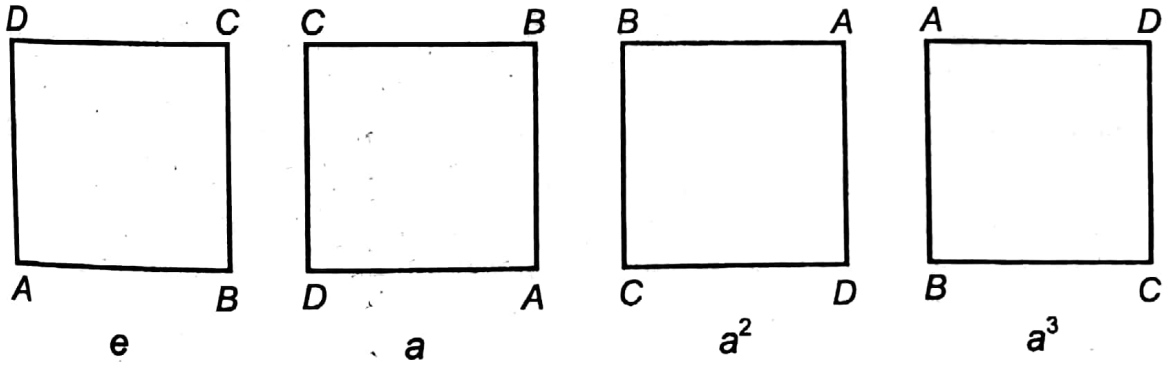
Each of the above motion is a single motion.

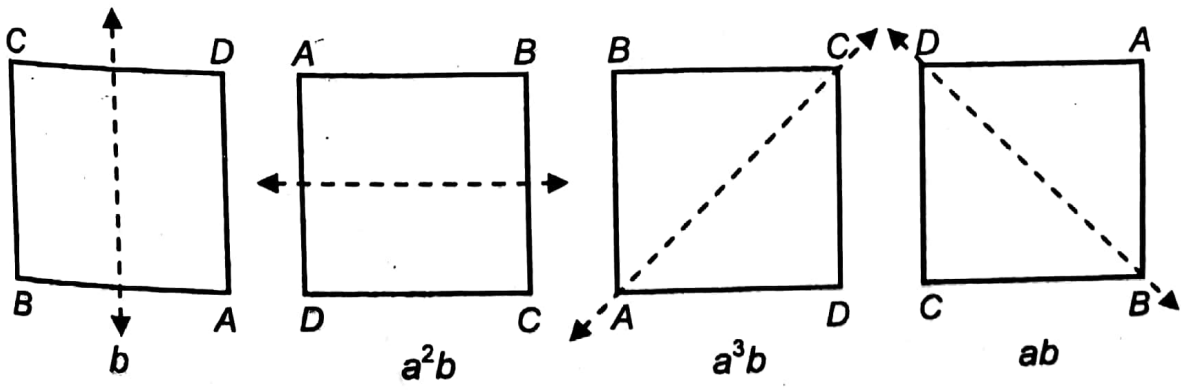
It is clear from above squares that:

(i) square x is obtained if we rotate square b counter clockwise through 180°, so $x = a^2b$.

(ii) square y is obtained if we rotate square b counter clockwise through 270°, so $y = a^3b$.

(iii) square z is obtained if we rotate square b counter clockwise through 90°, so $z = ab$.





The corresponding Cayley table is given below:

•	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Table-4: Cayley table of symmetry group of square

The symmetry group of a square is also known as *dihedral group* D_4. Thus the dihedral group D_4 is

$$D_4 = \{ e, a, a^2, a^3, b, ab, a^2b, a^3b \}$$

In the following we give another way of writing D_4 group:

$$D_4 = < a, b : a^4 = b^2 = (ab)^2 = e >$$

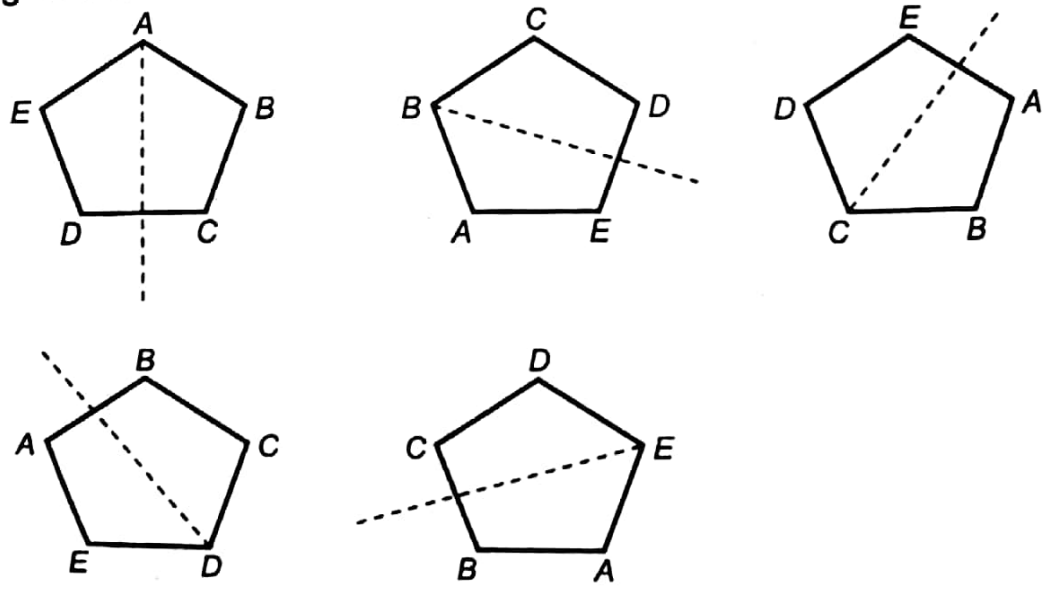
4-5 The Symmetry Group of a Regular Pentagon

In this section, first we find the axes of symmetry of a regular pentagon, then we shall find the symmetry group of pentagon.

4-5.1 Example: *Find the axes of reflection symmetry of a pentagon and show that it has 5-fold symmetry.*

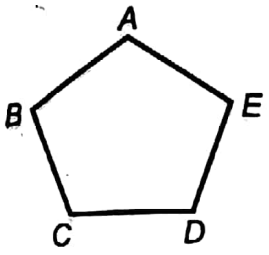
Solution: The rotational symmetries of the pentagon can be thought of as the rotations that leave the pentagon invariant.

In the following, we see that there are five lines over which the pentagon can be reflected and maintain its original appearance, so a pentagon has five axes of reflection symmetry.

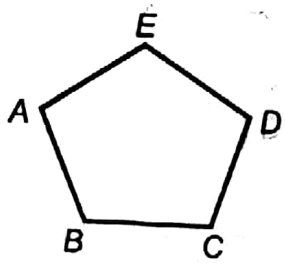


A pentagon is symmetric under those rotations which are equivalent to $\frac{1}{5}$ of a full rotation, i.e. $\frac{1}{5}(360°)$ or 72°.

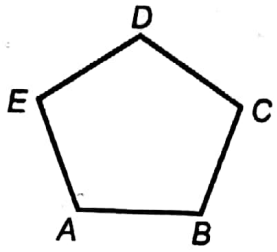
In the following we show the counter clockwise rotations of pentagon *ABCDE*.



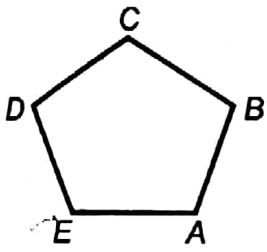
Initial Position



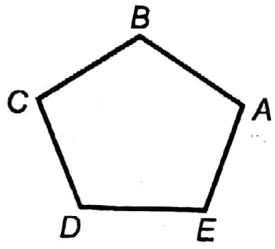
First Rotation of 72°



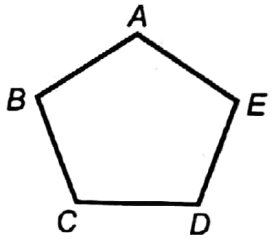
Second Rotation of 72°



Third Rotation of 72°



Fourth Rotation of 72°



Fifth Rotation of 72°
= Initial Position

This shows that the pentagon has a rotational symmetry of order 5 or 5-fold symmetry.

The Symmetry Group of the Pentagon / Dihedral Group D_5:

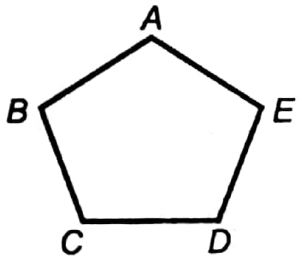
There are ten motions that can bring a pentagon back into its original position. They are

- Do nothing
- Rotate counter clockwise through 72°
- Rotate counter clockwise through 144°
- Rotate counter clockwise through 216°
- Rotate counter clockwise through 288°
- Flip about the symmetry axis (through vertex *A*)
- Flip about the symmetry axis (through vertex *B*)
- Flip about the symmetry axis (through vertex *C*)
- Flip about the symmetry axis (through vertex *D*)
- Flip about the symmetry axis (through vertex *E*)

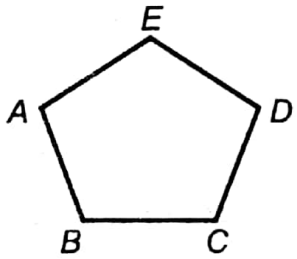
We use the following symbols to stand for our movements.

- ***e*** stands for the **Do nothing** movement.
- ***a*** stands for **Rotate** counter clockwise through **72°**.
- a^2 stands for **Rotate** counter clockwise through **144°**.
- a^3 stands for **Rotate** counter clockwise through **216°**.
- a^4 stands for **Rotate** counter clockwise through **288°**.
- ***b*** stands for **Flip** about the symmetry axis **(through vertex *A*)**.
- ***x*** stands for **Flip** about the symmetry axis **(through vertex *B*)**.
- ***y*** stands for **Flip** about the symmetry axis **(through vertex *C*)**.
- ***z*** stands for **Flip** about the symmetry axis **(through vertex *D*)**.
- ***t*** stands for **Flip** about the symmetry axis **(through vertex *E*)**.

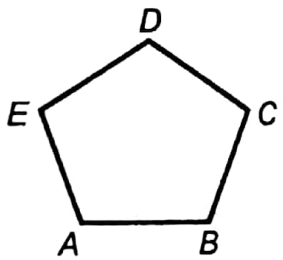
In order to complete Cayley table, first we write the following pentagons using the definitions of **e**, ***a***, a^2, a^3, a^4, ***b***, ***x***, ***y***, ***z*** and ***t***:



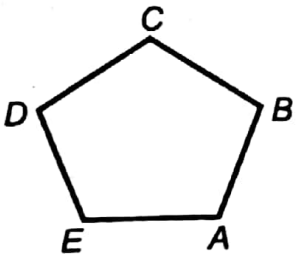
e



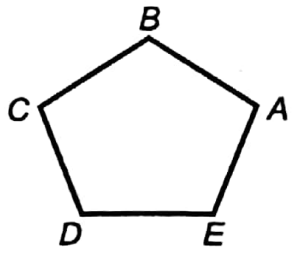
a



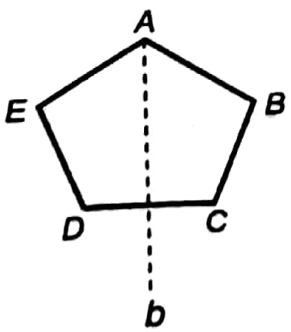
a^2



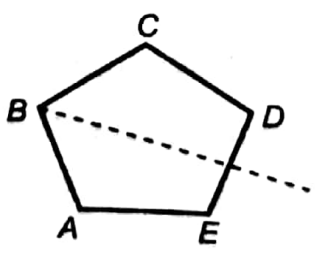
a^3



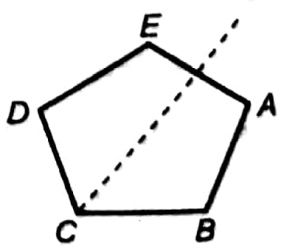
a^4



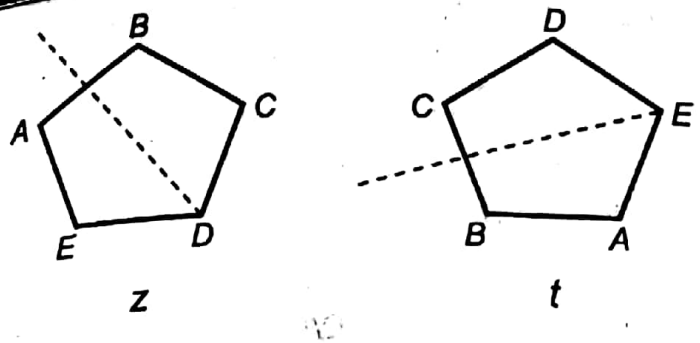
b



x



y



Each of the above motion is a single motion.
It is clear from above pentagons that:

(i) pentagon x is obtained if we rotate pentagon b counter clockwise through 144°, so $x = a^2b$.

(ii) pentagon y is obtained if we rotate pentagon b counter clockwise through 288°, so $y = a^4b$.

(iii) pentagon z is obtained if we rotate pentagon b counter clockwise through 72°, so $z = ab$.

(iv) pentagon t is obtained if we rotate pentagon b counter clockwise through 216°, so $t = a^3b$.

This shows that symmetric pentagons are

$$e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b$$

The corresponding Cayley table is given below:

$\cdot$	e	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
e	e	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
a	a	a^2	a^3	a^4	e	ab	a^2b	a^3b	a^4b	b
a^2	a^2	a^3	a^4	e	a	a^2b	a^3b	a^4b	b	ab
a^3	a^3	a^4	e	a	a^2	a^3b	a^4b	b	ab	a^2b
a^4	a^4	e	a	a^2	a^3	a^4b	b	ab	a^2b	a^3b
b	b	a^4b	a^3b	a^2b	ab	e	a^4	a^3	a^2	a
ab	ab	b	a^4b	a^3b	a^2b	a	e	a^4	a^3	a^2
a^2b	a^2b	ab	b	a^4b	a^3b	a^2	a	e	a^4	a^3
a^3b	a^3b	a^2b	ab	b	a^4b	a^3	a^2	a	e	a^4
a^4b	a^4b	a^3b	a^2b	ab	b	a^4	a^3	a^2	a	e

Table-5: Cayley table of symmetry group of regular pentagon

The symmetry group of a pentagon is also known as *dihedral group* D_5 Thus the dihedral group D_5 is

$$D_5 = \{ e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b \}$$

In the following we give another way of writing D_5 group:

$$D_5 = < a, b : a^5 = b^2 = (ab)^2 = e >$$

EXERCISE 4

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) The ideal sea star has _____ symmetry.
(a) 2-fold (b) 3-fold (c) 4-fold (d) 5-fold
ⓐ ⓑ ⓒ ⓓ

(ii) The butterfly has _____ symmetry.
(a) 2-fold (b) 3-fold (c) 4-fold (d) 5-fold
ⓐ ⓑ ⓒ ⓓ

(iii) An equilateral triangle has _____ symmetry.
(a) 2-fold (b) 3-fold (c) 4-fold (d) 5-fold
ⓐ ⓑ ⓒ ⓓ

(iv) A rectangle has _____ symmetry.
(a) 2-fold (b) 3-fold (c) 4-fold (d) 5-fold
ⓐ ⓑ ⓒ ⓓ

(v) The dihedral group D_6 has _____ proper subgroups.
(a) 5 (b) 4 (c) 3 (d) 2
ⓐ ⓑ ⓒ ⓓ

(vi) The Klein 4-group V_4 has _____ proper subgroups.
(a) 5 (b) 4 (c) 3 (d) 2
ⓐ ⓑ ⓒ ⓓ

(vii) The square has _____ symmetry.
(a) 2-fold (b) 3-fold (c) 4-fold (d) 5-fold
ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.2 Solve / answer the following short questions:

(i) Explain mirror symmetry.

(ii) Define rotational symmetry and its order.

(iii) Find the proper subgroups of dihedral group D_6.

Long Questions

Q.3 Explain the group of symmetries of a rectangle. PU, 2013 (M.Sc. Math)

Q.4 Explain the group of symmetries of a square.

Q.5 Explain the group of symmetries of an equilateral triangle.

SUMMARY

- The axis of symmetry separates the two halves and, if we place a mirror along this line, the design seems complete.
- Butterflies exhibit mirror symmetry.
- In general, bilateral symmetry is present whenever an object or design can be broken down into two parts, one of which is the reflection of the other.
- An object that exhibits rotational symmetry will appear unchanged if it is rotated through some angle.
- The number of rotations required for all the points to actually return to their original positions is called the order or degree of the rotation.
- An equilateral triangle has three axes of reflectional symmetry.
- The equilateral triangle has a rotational symmetry of order 3 or 3-fold symmetry.
- There are four proper subgroups of dihedral group D_6.
- The rectangle has two axes of reflection symmetry.
- The rectangle has a rotational symmetry of order 2 or 2-fold symmetry.
- V_4 has three proper subgroups.
- A square has four axes of reflection symmetry.
- The square has a rotational symmetry of order 4 or 4-fold symmetry.
- The regular pentagon has five axes of reflection symmetry.
- The regular pentagon has a rotational symmetry of order 5 or 5-fold symmetry.

- $V_4 = < a,b : a^2 = b^2 = (ab)^2 = e >$

  $= \{e, a, b, ab\}$

- $S_3 = < a,b : a^3 = b^2 = (ab)^2 = e >$

  $= \{e, a, a^2, b, ab, a^2b\}$

- $D_4 = < a,b : a^4 = b^2 = (ab)^2 = e >$

  $= \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

- $D_5 = < a,b : a^5 = b^2 = (ab)^2 = e >$

  $= \{e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$

*****

Chapter 5

HOMOMORPHISMS

In this chapter we shall be concerned with the definitions and results of group homomorphism. We shall also state and prove Cayley's theorem.

5-1 Homomorphism

In this section, we shall discuss some relation between groups.

5-1.1 Definition:

An element of order 2 in a group G is called an *involution*.

5-1.2 Theorem:

A group of even order contains at least one involution.

PU, 2013; 2010, 2002 (M.Sc. Math)

Proof: Let G be a group of even order and

$$A = \{x \in G : x^2 = e\}$$

$$B = \{y \in G : y^2 \neq e\}$$

Then obviously

$$G = A \cup B$$

and

$$A \cap B = \phi$$

There are two possible cases.

Case-I: If $B = \phi$, then $G = A$.

Hence G contains at least one involution.

Case-II: If $B \neq \phi$, then $y \in B$.

$$y^2 \neq e$$
$$\Rightarrow y.y \neq e$$
$$\Rightarrow y^{-1}.(y.y) \neq y^{-1}.e$$
$$\Rightarrow (y^{-1}y).y \neq y^{-1}$$
$$\Rightarrow e.y \neq y^{-1}$$
$$\Rightarrow y \neq y^{-1}$$
$$\Rightarrow y^{-1}.y \neq y^{-1}.y^{-1}$$
$$\Rightarrow e \neq (y^{-1})^2$$
$$\Rightarrow y^{-1} \in B$$

Since $e \notin B$ and $y^{-1} \in B$ for all $y \in B$, so B is a set of even order.

Since $A \cap B = \phi$ and $G = A \cup B$, so

$$|G| = |A| + |B| \qquad ...(1)$$

Since both G and B are of even order, so from (1), A must be of even order, i.e. is order of A must be at least 2.

Since A consists of elements x such that $x^2 = e$ and $e^2 = e$, so A contains e and at least one element x different from e, i.e.

$$x \in A,\ x^2 = e,\ x \neq e$$

Since A is a subset of G, so G contains at least one x such that $x \neq e$ and $x^2 = e$. Hence G contains at least on involution.

This completes the proof.

5-1.3 Definition:

Let $(G,\cdot)$ and $(G',*)$ be two groups. A mapping $\phi : G \to G'$ is said to be a *homomorphism* if for all $a,b \in G$

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

In other words, if there is no danger of confusion in the binary operations used in groups G and G', we can define homomorphism alternatively as follows:

A mapping ϕ from a group G into a group G' is said to be a *homomorphism* if for all $a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

5-1.4 Definition:

An onto homomorphism is called an *epimorphism*.

5-1.5 Definition:

A one-one homomorphism is called a *monomorphism*.

5-1.6 Definition:
A bijective homomorphism is called an *isomorphism*.

5-1.7 Definition:
Two groups G and G' are said to be *isomorphic* if there is an isomorphism $\phi : G \to G'$. In this case we write $G \approx G'$.

5-1.8 Definition:
A homomorphism from a group G to itself is called an *endomorphism* of G.

5-1.9 Definition:
An isomorphism from a group G to itself is called an *automorphism* of G.

5-1.10 Example:
Show that the mapping $\phi : G \to G$ *defined by*

$$\phi(x) = e \text{ for all } x \in G$$

where e is an identity element of G, is a homomorphism.

Solution:
Let $x, y \in G$, then using the definition of ϕ, we have

$$\begin{aligned} \phi(xy) &= e \\ &= ee && \because e = ee \\ &= \phi(x)\phi(y) && \because \phi(x) = e,\ \phi(y) = e \end{aligned}$$

This shows that ϕ is a homomorphism.

5-1.11 Example:
Show that the mapping $\phi : G \to G$ *defined by*

$$\phi(x) = x \text{ for all } x \in G$$

is a homomorphism.

Solution:
Let $x, y \in G$, then using the definition of ϕ, we have

$$\begin{aligned} \phi(xy) &= xy \\ &= \phi(x)\phi(y) && \because \phi(x) = x,\ \phi(y) = y \end{aligned}$$

This shows that ϕ is a homomorphism.

5-1.12 Example: *Let G be the group of all real numbers under addition and let G′ be the group of nonzero real numbers with the product being ordinary multiplication of real numbers. Define* $\phi : G \to G'$ *by* $\phi(x) = 2^x$. *Show that* ϕ *is a homomorphism from G into G′. Is* ϕ *onto?*

Solution:
Let $x, y \in G$, then using the definition of ϕ, we have

$$\phi(x+y) = 2^{x+y}$$
$$= 2^x 2^y$$
$$= \phi(x)\phi(y) \quad \because \phi(x) = 2^x, \phi(y) = 2^y$$

This shows that ϕ is a homomorphism from G into G'.

Since G' consists of nonzero real numbers, and 2^x is always a positive real number, so negative real numbers of G' are not images of elements of G under ϕ, i.e. G' is not an image of ϕ. This shows that ϕ is not onto.

5-1.13 Example:

Let $(R^+,\cdot)$ and $(R,+)$ be two groups. Define $\phi: R^+ \to R$ by $\phi(x) = \ln x$. Show that ϕ is an isomorphism.

Solution: (i) Well defined

First we show that ϕ is well defined, for this let

$$x = y$$
$$\Rightarrow \ln x = \ln y$$
$$\Rightarrow \phi(x) = \phi(y)$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

Since for every $\ln x \in R$, there is some positive real number x, i.e. $x \in R^+$ such that $\phi(x) = \ln x$.

This shows that ϕ is onto.

(iii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(x) = \phi(y)$$
$$\Rightarrow \ln x = \ln y$$
$$\Rightarrow e^{\ln x} = e^{\ln y}$$
$$\Rightarrow x = y$$

This shows that ϕ is one-one.

(iv) Homomorphism

In order to prove that ϕ is a homomorphism, let $x, y \in R^+$ and consider

$$\phi(x.y) = \ln(x.y)$$
$$= \ln x + \ln y$$
$$= \phi(x) + \phi(y)$$

This shows that ϕ is a homomorphism.

Hence, ϕ is an isomorphism.

5-1.14 Example:

Let G be the group of integers under addition. For the integer $x \in G$ define ϕ by $\phi(x) = 2x$. Show that $\phi : G \to G$ is a homomorphism.

Solution:

Let $x, y \in G$ and consider

$$\begin{aligned}\phi(x+y) &= 2(x+y)\\ &= 2x+2y\\ &= \phi(x)+\phi(y)\end{aligned}$$

This shows that ϕ is a homomorphism.

5-1.15 Example:

Let G be the group of nonzero real numbers under multiplication and $G' = \{1, -1\}$ a group under multiplication. For $x \in G$, define $\phi : G \to G'$ by

$$\phi(x) = \begin{cases} 1 & \text{if} \quad x > 0 \\ -1 & \text{if} \quad x < 0 \end{cases}$$

Show that ϕ is a homomorphism.

Solution:

Let $x, y \in G$ and consider

$$\phi(xy) = \begin{cases} 1 & \text{if} \quad xy > 0 \\ -1 & \text{if} \quad xy < 0 \end{cases}$$

$$= \begin{cases} \begin{cases} 1 & \text{if} \quad x > 0, y > 0 \\ 1 & \text{if} \quad x < 0, y < 0 \end{cases} \\ \begin{cases} -1 & \text{if} \quad x > 0, y < 0 \\ -1 & \text{if} \quad x < 0, y > 0 \end{cases} \end{cases}$$

$$= \begin{cases} \begin{cases} 1.1 & \text{if} \quad x > 0, y > 0 \\ (-1).(-1) & \text{if} \quad x < 0, y < 0 \end{cases} \\ \begin{cases} 1.(-1) & \text{if} \quad x > 0, y < 0 \\ (-1).1 & \text{if} \quad x < 0, y > 0 \end{cases} \end{cases}$$

$$= \begin{cases} \begin{cases} \phi(x)\phi(y) & \text{if} \quad x > 0, y > 0 \\ \phi(x)\phi(y) & \text{if} \quad x < 0, y < 0 \end{cases} \\ \begin{cases} \phi(x)\phi(y) & \text{if} \quad x > 0, y < 0 \\ \phi(x)\phi(y) & \text{if} \quad x < 0, y > 0 \end{cases} \end{cases}$$

$$= \phi(x)\phi(y)$$

This shows that ϕ is a homomorphism.

5-1.16 Example:

Let G be the group of all real 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad-bc\neq 0$, under matrix multiplication. Let G' be the group of all nonzero real numbers under multiplication. Define $\phi: G \to G'$ by

$$\phi\begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad-bc$$

Show that ϕ is a homomorphism.

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in G$, then by definition of G, we have

$$ad-bc\neq 0 \quad ...(1) \qquad a'd'-b'c'\neq 0 \quad ...(2)$$

Now

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$$

$$\Rightarrow \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = \phi\begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$$

$$\begin{aligned} &= (aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc') \\ &= aa'cb' + aa'dd' + bc'cb' + bc'dd' \\ &\quad -(ab'ca' + ab'dc' + bd'ca' + bd'dc') \\ &= aa'dd' + bb'cc' - adb'c' - bca'd' \\ &= ada'd' - adb'c' + bcb'c' - bca'd' \\ &= ad(a'd'-b'c') - bc(a'd'-b'c') \\ &= (ad-bc)(a'd'-b'c') \\ &= \phi\begin{bmatrix} a & b \\ c & d \end{bmatrix}\phi\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \end{aligned}$$

This shows that ϕ is a homomorphism.

5-1.17 Theorem:

If $\phi: G \to G'$ is a homomorphism of G into G', then

(a) $\phi(e) = e'$, *where $e' \in G'$ is an identity element of G'*

(b) $\phi(x^{-1}) = \phi(x)^{-1}$ *for all $x \in G$*

Proof: (a) Using the definition of homomorphism ϕ, we have

$$\phi(x) = \phi(x.e) = \phi(x)\phi(e) \qquad \phi(x) = \phi(e.x) = \phi(e)\phi(x)$$

This shows that $\phi(e)$ is an identity element of G', so $\phi(e) = e'$.

(b) For any $x \in G$, consider

$$\begin{aligned}\phi(x)\phi(x^{-1}) &= \phi(x.x^{-1}) \\ &= \phi(e) && \because x.x^{-1} = e \\ &= e' && \because \phi(e) = e'\end{aligned}$$

Similarly,

$$\begin{aligned}\phi(x^{-1})\phi(x) &= \phi(x^{-1}.x) \\ &= \phi(e) && \because x^{-1}.x = e \\ &= e' && \because \phi(e) = e'\end{aligned}$$

This shows that $\phi(x^{-1})$ is the inverse of $\phi(x)$, i.e. $\phi(x^{-1}) = \phi(x)^{-1}$.

This completes the proof.

5-1.18 Symmetric Group S_3:

In chapter 3, we have already proved the symmetric group S_3 consisting of permutations

$$I = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \quad f_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \quad f_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$f_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \quad f_4 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \quad f_5 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

in a set $X = \{1,2,3\}$.

In the rest of our discussion, we shall rename above permutations as follows:

First we write the three basic permutations in which we take an identity permutation, a cycle of length 2, (1, 2) and a cycle of length 3, (1, 2, 3), i.e.

$$e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \qquad \text{(Not a cycle)}$$

$$\phi = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \qquad \text{(A cycle of length 2)}$$

$$\psi = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \qquad \text{(A cycle of length 3)}$$

Now the remaining three permutations can be obtained using ϕ and ψ, i.e.

$$\psi^2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$\phi\psi = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

$$\phi\psi^2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

Thus, the symmetric group S_3 has the elements $e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2$, i.e.

$$S_3 = \{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$$

5-1.19 Example:

Let $S_3 = \{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$ and $G' = \{e, \phi\}$. Define the mapping $f : S_3 \to G'$ by $f(\phi^i\psi^j) = \phi^i$. Show that f is a homomorphism.

Solution: It is clear from the definition of f that

$$f(e) = e,\ f(\phi) = \phi,\ f(\psi) = e,\ f(\psi^2) = e,\ f(\phi\psi) = \phi,\ f(\phi\psi^2) = \phi$$

This shows that

$$\begin{aligned} f(\phi^i\psi^j) &= \phi^i \\ &= \phi^i e \qquad \because \phi^i = \phi^i e \\ &= f(\phi^i)f(\psi^j) \quad \because f(\phi^i) = \phi^i,\ f(\psi^j) = \psi^j \end{aligned}$$

This shows that f is a homomorphism.

5-1.20 Example:

Let G be any abelian group, and $\phi : G \to G$ is defined by $\phi(x) = x^5$ for all $x \in G$. Show that ϕ is a homomorphism.

Solution: Let $x, y \in G$, then using the definition of ϕ, we have

$$\begin{aligned} \phi(xy) &= (xy)^5 \\ &= x^5y^5 \quad \because G \text{ is abelian } \therefore (xy)^5 = x^5y^5 \\ &= \phi(x)\phi(y) \end{aligned}$$

This shows that ϕ is a homomorphism.

5-1.21 Example: *Let G be any group, g a fixed element in G. Define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$ for all $x \in G$. Prove that ϕ is an isomorphism.*

Solution: **(i) Well defined**

First we show that ϕ is well defined, for this let

$$\begin{aligned} & x = y \\ \Rightarrow\ & gx = gy \\ \Rightarrow\ & gxg^{-1} = gyg^{-1} \\ \Rightarrow\ & \phi(x) = \phi(y) \end{aligned}$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

Since for every $gxg^{-1} \in G$, there is some $x \in G$ such that

$$\phi(x) = gxg^{-1}$$

This shows that ϕ is onto, i.e. ϕ is an epimorphism.

(iii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(x) = \phi(y)$$
$$\Rightarrow gxg^{-1} = gyg^{-1}$$
$$\Rightarrow g^{-1}(gxg^{-1})g = g^{-1}(gyg^{-1})g$$
$$\Rightarrow g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$$
$$\Rightarrow exe = eye \qquad \because g^{-1}g = e$$
$$\Rightarrow x = y$$

This shows that ϕ is one-one, i.e. ϕ is a monomorphism.

(iv) Homomorphism

In order to prove that ϕ is a homomorphism, let $x, y \in G$, then using the definition of ϕ, we have

$$\phi(xy) = gxyg^{-1}$$
$$= gxeyg^{-1}$$
$$= gxg^{-1}gyg^{-1} \qquad \because g^{-1}g = e$$
$$= (gxg^{-1})(gyg^{-1})$$
$$= \phi(x)\phi(y)$$

This shows that ϕ is a homomorphism.

Hence, ϕ is an isomorphism.

5-1.22 Theorem: *If G is a group and a mapping $\phi: G \to G$, defined by $\phi(x) = x^{-1}$ for all $x \in G$, is a homomorphism, then G is abelian.*

Proof: Let $x, y \in G$, then

$$xy = (y^{-1}x^{-1})^{-1}$$
$$= \phi(y^{-1}x^{-1})$$
$$= \phi(y^{-1})\phi(x^{-1}) \qquad \because \phi \text{ is homomorphi sm}$$
$$= yx$$

This shows that G is an abelian group. This completes the proof.

5-1.23 Example: *Let ϕ be a mapping from $(Z,+)$ the group of integers to the group $G = \{1,-1\}$ under multiplication defined as $\phi: Z \to G$ such that*

$$\phi(x) = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$$

Show that ϕ is a homomorphism. Is ϕ an isomorphism?

Solution:

Let $x, y \in Z$, then using the definition of ϕ, we have

$$\phi(x+y) = \begin{cases} 1 & \text{if } x+y \text{ is even} \\ -1 & \text{if } x+y \text{ is odd} \end{cases}$$

$$= \begin{cases} \begin{cases} 1 & \text{if both } x \text{ and } y \text{ are even} \\ 1 & \text{if both } x \text{ and } y \text{ are odd} \end{cases} \\ \begin{cases} -1 & \text{if } x \text{ is even } y \text{ is odd} \\ -1 & \text{if } x \text{ is odd } y \text{ is even} \end{cases} \end{cases}$$

$$= \begin{cases} \begin{cases} 1.1 & \text{if both } x \text{ and } y \text{ are even} \\ (-1).(-1) & \text{if both } x \text{ and } y \text{ are odd} \end{cases} \\ \begin{cases} 1.(-1) & \text{if } x \text{ is even } y \text{ is odd} \\ (-1).1 & \text{if } x \text{ is odd } y \text{ is even} \end{cases} \end{cases}$$

$$= \begin{cases} \begin{cases} \phi(x)\phi(y) & \text{if both } x \text{ and } y \text{ are even} \\ \phi(x)\phi(y) & \text{if both } x \text{ and } y \text{ are odd} \end{cases} \\ \begin{cases} \phi(x)\phi(y) & \text{if } x \text{ is even } y \text{ is odd} \\ \phi(x)\phi(y) & \text{if } x \text{ is odd } y \text{ is even} \end{cases} \end{cases}$$

$$= \phi(x)\phi(y)$$

This shows that ϕ is a homomorphism.

Since both 2 and 4 are even integers, so by the definition of ϕ, we have

$$\phi(2) = 1 = \phi(4)$$

This shows that two different element have same image, so ϕ is not one-one. Hence ϕ is not an isomorphism.

5-1.24 Definition (Kernel of Homomorphism):

Let ϕ be a homomorphism of G into G' and e' be an identity element of G', the *kernel of* ϕ is denoted by K_ϕ and is defined as

$$K_\phi = \{x \in G : \phi(x) = e'\}$$

In other words, the *kernel of homomorphism* $\phi : G \to G'$ is the set of those elements of G whose image is the identity element of G'.

K_ϕ is also denoted by $Ker\phi$.

5-1.25 Theorem: *A homomorphism $\phi : G \to G'$ is one-one if and only if $Ker\phi = \{e\}$.*

PU, 2007 (M.Sc. Math)

Proof: Let ϕ one-one. Let $x \in Ker\phi$, then by the definition of kernel of homomorphism, we have

$$\phi(x) = e' \qquad \ldots(1)$$

where e' is the identity element of G'.

The image of identity element e is the identity element e', i.e.

$$\phi(e) = e' \qquad \ldots(2)$$

Equating (1) and (2), we have

$$\phi(x) = \phi(e)$$

$$\Rightarrow x = e \qquad \because \phi \text{ is one - one}$$

This shows that $Ker\phi$ contains only e, i.e $Ker\phi = \{e\}$

Conversely, let $Ker\phi$ contain only e, i.e. $Ker\phi = \{e\}$.

Next consider

$$\phi(x) = \phi(y)$$

$$\Rightarrow \phi(x)\phi(y)^{-1} = e'$$

$$\Rightarrow \phi(x)\phi(y^{-1}) = e' \qquad \because \phi(y)^{-1} = \phi(y^{-1})$$

$$\Rightarrow \phi(xy^{-1}) = e' \qquad \because \phi \text{ is homomorphi sm}$$

$$\Rightarrow xy^{-1} \in Ker\phi$$

$$\Rightarrow xy^{-1} = e \qquad \because Ker\phi = \{e\}$$

$$\Rightarrow x = y$$

This shows that ϕ is one-one. This completes the proof.

5-1.26 Theorem: *Let $\phi : G \to G'$ be a homomorphism of a group G onto another group G'. The homomorphic image $\phi(G)$ of the group G is itself a group.*

PU, 2009 (M.Sc. Math)

Proof:

G_1): Let $\phi(x), \phi(y) \in \phi(G)$, then $x, y \in G$.

Since G is a group, so for $x, y \in G$

$$xy \in G$$

$$\Rightarrow \phi(xy) \in \phi(G)$$

$$\Rightarrow \phi(x)\phi((y) \in \phi(G) \qquad \because \phi \text{ is a homomorphi sm}$$

This shows that closure law holds in $\phi(G)$.

G_2): Since $\phi(G) \subset G'$ and G', so associative law holds in $\phi(G)$.

G_3): If e is the identity element of G, then $e \in G$, so $\phi(e) \in \phi(G)$.

Using the definition of homomorphism ϕ, we have

$$\phi(x) = \phi(x.e) = \phi(x)\phi(e) \quad \Big| \quad \phi(x) = \phi(e.x) = \phi(e)\phi(x)$$

This shows that $\phi(e)$ is an identity element of $\phi(G)$, so the identity element exists in $\phi(G)$.

G_4): Let $\phi(x) \in \phi(G)$, then $x \in G$.

Using the definition of homomorphism, we have

$$\phi(x)\phi(x^{-1}) = \phi(x.x^{-1})$$
$$= \phi(e) \qquad \because x.x^{-1} = e$$

Similarly,

$$\phi(x^{-1})\phi(x) = \phi(x^{-1}.x)$$
$$= \phi(e) \qquad \because x^{-1}.x = e$$

This shows that $\phi(x^{-1})$ is the inverse of $\phi(x)$. Since G is a group, so for $x \in G$, we have

$$x^{-1} \in G$$
$$\Rightarrow \phi(x^{-1}) \in \phi(G)$$

This shows that the inverse of each element of $\phi(G)$ is in $\phi(G)$. Hence $\phi(G)$ is itself a group.

5-1.27 Theorem: *Let $\phi : G \to G'$ be a homomorphism of a group G onto another group G', then $|\phi(a)| = |a|$ for $a \in G$.*

Proof: If e is the identity element of G, then $e \in G$, so $\phi(e) \in \phi(G)$.

Using the definition of homomorphism ϕ, we have

$$\phi(x) = \phi(x.e) \quad | \quad \phi(x) = \phi(e.x)$$
$$= \phi(x)\phi(e) \quad | \quad = \phi(e)\phi(x)$$

This shows that $\phi(e)$ is an identity element of $\phi(G)$.

Let $$|a| = n \qquad ...(1)$$

Then, by the definition of order of an element of a group, we have

$$a^n = e$$
$$\Rightarrow \phi(a^n) = \phi(e)$$
$$\Rightarrow \phi(a \cdot a \cdot \ldots a) = \phi(e)$$
$$\Rightarrow \phi(a) \cdot \phi(a) \cdot \ldots \phi(a) = \phi(e) \qquad \because \phi \text{ is a homomorphi sm}$$
$$\Rightarrow (\phi(a))^n = \phi(e)$$
$$\Rightarrow |\phi(a)| = n \qquad ...(2)$$

Equating (1) and (2), we have

$$|\phi(a)| = |a|$$

5-1.28 Theorem: *The homomorphic image of a cyclic group is cyclic.*

Proof: Let G be a cyclic group generated by a.

Let $\phi: G \to G'$ be homomorphism. Then we have to show that the homomorphic image $\phi(G)$ of G is cyclic. For this, let $x \in \phi(G)$ be any element of $\phi(G)$, then there must be an element of G whose image under ϕ is x. Since G is cyclic group generated by a, so each element of G must be some power of a.

Consequently, for some positive integer k, we have

$$\begin{aligned} x &= \phi(a^k) \\ &= \phi(a \cdot a \cdot \ldots \cdot a) \\ &= \phi(a) \cdot \phi(a) \cdot \ldots \cdot \phi(a) \qquad \because \phi \text{ is a homomorphism} \\ &= (\phi(a))^k \end{aligned}$$

This shows that x is a power of $\phi(a)$. Similarly, we can show that each element of $\phi(G)$ is some power of $\phi(a)$, so $\phi(a)$ is a generator of $\phi(G)$. Hence $\phi(G)$ is a cyclic group generated by $\phi(a)$.

5-1.29 Theorem:

Any two cyclic groups of the same order are isomorphic.

PU, 2015 (BS Math); PU, 2012; 2010 (M.Sc. Math)

Proof: Let G and G' be any two cyclic groups of the same finite order n, i.e.

$$|G| = n$$

and

$$|G'| = n$$

Let G be generated by a, i.e.

$$G = < a : a^n = e >$$

Let us consider another group

$$C_n = \left\{ z \in C : z = e^{\frac{2k\pi i}{n}} \right\}$$

where k is an integer. Then obviously C_n is a cyclic group of order n generated by $e^{\frac{2k\pi i}{n}}$, because $(e^{\frac{2k\pi i}{n}})^n = e^{2k\pi i} = 1$.

Next we define a mapping $\phi: G \to C_n$ by

$$\phi(a^k) = e^{\frac{2k\pi i}{n}}$$

(i) Well defined

Let

$$a^k = a^l$$

$$\Rightarrow a^{k-l} = e$$

Which is only possible if $k - l = 0$, i.e.

$$k = l$$

$$\Rightarrow \frac{2k\pi i}{n} = \frac{2l\pi i}{n}$$

$$\Rightarrow e^{\frac{2k\pi i}{n}} = e^{\frac{2l\pi i}{n}}$$

$$\Rightarrow \phi(a^k) = \phi(a^l)$$

This shows that ϕ is well defined.

(ii) One-One

$$\Rightarrow \phi(a^k) = \phi(a^l)$$

$$\Rightarrow e^{\frac{2k\pi i}{n}} = e^{\frac{2l\pi i}{n}}$$

$$\Rightarrow \ln e^{\frac{2k\pi i}{n}} = \ln e^{\frac{2l\pi i}{n}}$$

$$\Rightarrow \frac{2k\pi i}{n} \ln e = \frac{2l\pi i}{n} \ln e$$

$$\Rightarrow \frac{2k\pi i}{n} = \frac{2l\pi i}{n} \qquad \because \ln e = 1$$

$$\Rightarrow k = l$$

$$\Rightarrow a^k = a^l$$

This shows that ϕ is one-one.

(iii) Onto

For $e^{\frac{2k\pi i}{n}} \in C_n$, there is some $a^k \in G$ such that $\phi(a^k) = e^{\frac{2k\pi i}{n}}$, so every element of C_n is an image of some element of G, so ϕ is onto.

(iv) Homomorphism

$$\phi(a^k \cdot a^l) = \phi(a^{k+l})$$

$$= e^{\frac{2(k+l)\pi i}{n}}$$

$$= e^{\frac{2k\pi i}{n}} \cdot e^{\frac{2l\pi i}{n}}$$

$$= \phi(a^k) \cdot \phi(a^l)$$

This shows that ϕ is a homomorphism.

Since ϕ, being a bijective homomorphism, is an isomorphism, so G and C_n are isomorphic, i.e. $G \approx C_n$.

Similarly, we can show that $G' \approx C_n$.

Consequently, $G \approx G'$, i.e. G and G' are isomorphic.

5-1.30 Theorem: *Any two infinite cyclic groups are isomorphic.*

Proof: Let G and G' be any two infinite cyclic groups.

Let a be the generator of group G.

Let us consider another group $(Z,+)$, the group of integers under addition. Obviously, $(Z,+)$ is an infinite cyclic group.

For an integer k, let us define a mapping $\phi: G \to Z$ by

$$\phi(a^k) = k$$

(i) Well defined

Let $a^k = a^l$

$$a^{k-l} = e$$

Which is only possible if $k - l = 0$, i.e.

$$k = l$$

$$\Rightarrow \phi(a^k) = \phi(a^l)$$

This shows that ϕ is well defined.

(ii) One-One

$$\phi(a^k) = \phi(a^l)$$

$$\Rightarrow k = l$$

$$\Rightarrow a^k = a^l$$

This shows that ϕ is one-one.

(iii) Onto

For $k \in Z$, there is some $a^k \in G$ such that $\phi(a^k) = k$, so every element of Z is an image of some element of G, so ϕ is onto.

(iv) Homomorphism

$$\phi(a^k \cdot a^l) = \phi(a^{k+l})$$

$$= k + l$$

$$= \phi(a^k) + \phi(a^l)$$

This shows that ϕ is a homomorphism.

Since ϕ, being a bijective homomorphism, is an isomorphism, so G and Z are isomorphic, i.e. $G \approx Z$.

Similarly, we can show that $G' \approx Z$.

Consequently, $G \approx G'$, i.e. G and G' are isomorphic.

This completes the proof.

5-1.31 Example: *Let $\phi: G \to G'$ be an onto homomorphism and H be a subgroup of G. Show that $\phi(H)$ is a subgroup of G'.*

Solution: Let $x, y \in \phi(H)$, then there are $h_1, h_2 \in H$ such that

$$\phi(h_1) = x,\ \phi(h_2) = y$$

Since H is a subgroup, so

$$h_1, h_2 \in H$$

$$\Rightarrow h_1, h_2^{-1} \in H$$

Next consider

$$\begin{aligned} xy^{-1} &= \phi(h_1)(\phi(h_2))^{-1} \\ &= \phi(h_1)\phi(h_2^{-1}) && \because (\phi(h_2))^{-1} = \phi(h_2^{-1}) \\ &= \phi(h_1h_2^{-1}) && \because \phi \text{ is homomorphism} \\ &\in \phi(H) && \because h_1h_2^{-1} \in H \end{aligned}$$

This shows that $\phi(H)$ is a subgroup of G'.

5-1.32 Example: *Let $\phi : G \to G'$ be an onto homomorphism and H' be a subgroup of G'. Show that $\phi^{-1}(H')$ is a subgroup of G.*

Solution: Let $x, y \in \phi^{-1}(H')$, then

$$\begin{aligned} &\phi(x), \phi(y) \in H' \\ \Rightarrow\ &\phi(x)(\phi(y))^{-1} \in H' && \because H' \text{ is a subgroup} \\ \Rightarrow\ &\phi(x)\phi(y^{-1}) \in H' && \because (\phi(y))^{-1} = \phi(y^{-1}) \\ \Rightarrow\ &\phi(xy^{-1}) \in H' && \because \phi \text{ is homomorphism} \\ \Rightarrow\ &xy^{-1} \in \phi^{-1}(H') \end{aligned}$$

This shows that $\phi^{-1}(H')$ is a subgroup of G.

5-2 Cayley's Theorem

In this section we shall state and prove Cayley's theorem.

5-2.1 Definition: By *embedding* G into G', we mean that there is a subgroup of G' which is isomorphic to G.

5-2.2 Theorem (Cayley's Theorem):

Statements of Cayley's Theorem:

(i) *Every group is isomorphic to a subgroup of a symmetric group.*
(ii) *Every group is isomorphic to some permutation group.*
(iii) *Any group G can be embedded in a group of bijective mappings of a certain set.*

Proof: Let us define $\phi_g : G \to G$ by PU, 2015 (BS Math); PU, 2009; 2006 (M.Sc. Math)

$$\phi_g(x) = gx, \qquad \forall\, x \in G,\ g \in G$$

(i) Well defined
Let

$$\begin{aligned} &x = y \\ \Rightarrow\ &gx = gy \\ \Rightarrow\ &\phi_g(x) = \phi_g(y) \end{aligned}$$

This shows that ϕ_g is well defined.

(ii) One-One

$$\phi_g(x) = \phi_g(y)$$
$$\Rightarrow gx = gy$$
$$\Rightarrow x = y$$

This shows that ϕ_g is one-one.

(iii) Onto

For $gx \in G$, there is some $x \in G$ such that $\phi_g(x) = gx$, so every element of G is an image of some element of G, so ϕ_g is onto.

Hence, ϕ_g is a bijective mapping from G to G.

It is clear that ϕ_g, being a bijective mapping from G to G, is a permutation. Therefore, the set defined by

$$\Phi_G = \{\phi_g : g \in G\}$$

is a set of permutations.

Next we shall prove that Φ_G is a group.

G_1): Let $\phi_g, \phi_{g'} \in \Phi_G$, then, for $x \in G$, $\phi_g(x) = gx, \phi_{g'}(x) = g'x$

Now

$$\phi_g\phi_{g'}(x) = \phi_g(\phi_{g'}(x))$$
$$= \phi_g(g'x)$$
$$= gg'x$$
$$\Rightarrow \phi_g\phi_{g'} \in \Phi_G$$

This shows that closure law holds in Φ_G.

G_2): Let $\phi_g, \phi_{g'}, \phi_{g''} \in \Phi_G$, then for $x \in G$, we have

$$\phi_g(\phi_{g'}\phi_{g''})(x) = gg'g''x = (\phi_g\phi_{g'})\phi_{g''}(x)$$
$$\Rightarrow \phi_g(\phi_{g'}\phi_{g''}) = (\phi_g\phi_{g'})\phi_{g''}$$

This shows associative law holds in Φ_G.

G_3): If e is the identity element of G, then $e \in G$, so $\phi_e \in \Phi_e$ such that

$$\phi_e\phi_g(x) = \phi_e(\phi_g(x))$$
$$= \phi_e(gx)$$
$$= egx$$
$$= gx$$
$$= \phi_g(x)$$
$$\Rightarrow \phi_e\phi_g = \phi_g$$

$$\phi_g\phi_e(x) = \phi_g(\phi_e(x))$$
$$= \phi_g(ex)$$
$$= \phi_g(x)$$
$$\Rightarrow \phi_g\phi_e = \phi_g$$

This shows that ϕ_e is an identity element of Φ_e.

G_4): Since G is a group, so $g^{-1} \in G$ for $g \in G$, so $\phi_{g^{-1}} \in \Phi_e$ such that

$$\begin{aligned}\phi_g\phi_{g^{-1}}(x) &= \phi_g(\phi_{g^{-1}}(x)) \\ &= \phi_g(g^{-1}x) \\ &= gg^{-1}x \\ &= ex \\ &= \phi_e(x) \\ \Rightarrow \phi_g\phi_{g^{-1}} &= \phi_e\end{aligned}$$

$$\begin{aligned}\phi_{g^{-1}}\phi_g(x) &= \phi_{g^{-1}}(\phi_g(x)) \\ &= \phi_{g^{-1}}(gx) \\ &= g^{-1}gx \\ &= ex \\ &= \phi_e(x) \\ \Rightarrow \phi_{g^{-1}}\phi_g &= \phi_e\end{aligned}$$

This shows that $\phi_{g^{-1}}$ is the inverse of ϕ_g.

Hence, Φ_G is itself a group, so Φ_G is a group of permutations.

Finally, we shall prove that G is isomorphic to the group of permutations Φ_G. For this let us define $\psi : G \to \Phi_G$ by

$$\psi(g) = \phi_g$$

(i) Well defined

$$\begin{aligned}g &= g' \\ \Rightarrow gx &= g'x \\ \Rightarrow \phi_g(x) &= \phi_{g'}(x) \\ \Rightarrow \phi_g &= \phi_{g'} \\ \Rightarrow \psi(g) &= \psi(g')\end{aligned}$$

This shows that ψ is well defined.

(ii) One-One

$$\begin{aligned}\psi(g) &= \psi(g') \\ \Rightarrow \phi_g &= \phi_{g'} \\ \Rightarrow \phi_g(x) &= \phi_{g'}(x) \\ \Rightarrow gx &= g'x \\ \Rightarrow g &= g'\end{aligned}$$

This shows that ψ is one-one.

(iii) Onto

For $\phi_g \in \Phi_G$, there is some $g \in G$ such that $\psi(g) = \phi_g$, so every element of Φ_G is an image of some element of G, so ψ is onto.

Hence, ψ is a bijective mapping from G to Φ_G.

(iv) Homomorphism

For $g, g', x \in G$, we have

$$\phi_{gg'}(x) = gg'x$$

Similarly,

$$\phi_g\phi_{g'}(x) = \phi_g(\phi_{g'}(x))$$
$$= \phi_g(g'x)$$
$$= gg'x$$

Therefore, $\phi_{gg'} = \phi_g\phi_{g'}$

Next consider

$$\psi(gg') = \phi_{gg'}$$
$$= \phi_g\phi_{g'}$$
$$= \psi(g)\psi(g')$$

This shows that ψ is a homomorphism.

Thus, ψ, being bijective homomorphism, is an isomorphism.

This shows that $G \approx \Phi_G$, i.e. any group G is isomorphic to some permutation group Φ_G.

This completes the proof.

5-2.3 Theorem:

Let $G = < a : a^n = e >$ be a cyclic group, then a^m is a generator of G if and only if n and m are relatively prime.

PU, 2013; 2009 (M.Sc. Math)

Proof: Let a^m be the generator of G. Since $a \in G$, so there is some integer p such that

$$(a^m)^p = a$$
$$\Rightarrow a^{mp} = a$$
$$\Rightarrow a^{mp-1} = e$$
$$\Rightarrow mp - 1 > n$$
$$\Rightarrow n / mp - 1$$
$$\Rightarrow mp - 1 = nt \text{ for some integer } t$$
$$\Rightarrow pm + (-t)n = 1$$
$$\Rightarrow (m,n) = 1$$

This shows that n and m are relatively primes.

Conversely, let n and m are relatively primes, then there are integers p and q, such that

$$mp + nq = 1$$
$$\Rightarrow a^{mp+nq} = a^1$$
$$\Rightarrow a^{mp}a^{nq} = a$$
$$\Rightarrow (a^m)^p(a^n)^q = a$$
$$\Rightarrow (a^m)^p(e)^q = a \quad \because a^n = e$$

$$\Rightarrow (a^m)^p e = a \qquad \because (e)^q = e$$

$$\Rightarrow (a^m)^p = a$$

This shows that a^m is a generator of G.

5-2.4 Theorem:

Every group of prime order is cyclic and hence abelian.

PU, 2010 (M.Sc. Math)

Proof: Let G be a group of prime order p, then we have to show that G is cyclic. Let a be any non-identity element of G. Let H be a cyclic subgroup of G generated by a, then by Lagrange's theorem the order of H must divide the order p of G. Since p is prime, so the order of H is either 1 or p. But a is non-identity, so the order of H will not be 1. Therefore the order of H is p. This shows that

$$H = G$$

but the G is cyclic, because H is cyclic. Hence any group of prime order is cyclic.

Since every cyclic group is an abelian group, so G, being the cyclic group, is an abelian group.

5-2.5 Example:

Let $G = \langle x, y : x^3 = y^2 = xy = 1 \rangle$, *then show that* $G = \{1\}$.

PU, 2008; 2006; 2005; 2004 (M.Sc. Math)

Solution: As $xy = 1$

$$\Rightarrow y = x^{-1}$$

Similarly, $y^2 = xy$

$$\Rightarrow y^2 y^{-1} = (xy)y^{-1}$$

$$\Rightarrow y = x$$

and, $x^3 = y^2$

$$\Rightarrow x^3 = x^2 \qquad \because y = x$$

$$\Rightarrow x^3 x^{-2} = x^2 x^{-2}$$

$$\Rightarrow x = 1$$

$$\Rightarrow y = 1 \qquad \because y = x$$

Hence, $G = \{1\}$.

5-2.6 Example:

Prove that a non-commutative group has at least six elements.

PU, 2002; 2001 (M.Sc. Math)

Solution: Since group of order 1 consists of only identity element, so it is commutative (abelian).

Groups of orders 2 and 3 are abelian because 2 and 3 are relatively

prime numbers.

Group of order 4 is abeliab, because 4 is a square of 2 and 2 is a prime number.

Group of order 5 is abelian, because 5 is a prime number.

S_3 is a non-abilian group and its order is 6.

Hence, a non-commutative group has at least six elements.

EXERCISE 5

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) An element of order _____ in a group G is called an involution.

(a) 1 (b) 2 (c) 3 (d) 4

ⓐ ⓑ ⓒ ⓓ

(ii) A mapping ϕ from a group G into a group G' is said to be a homomorphism if for all $a, b \in G$, $\phi(ab) =$

(a) ab (b) a^2b^2

(c) $\phi(a)\phi(b)$ (d) $\phi(a+b)$

ⓐ ⓑ ⓒ ⓓ

(iii) A group of even order contains at least

(a) four involutions (b) three involutions

(c) two involutions (d) one involution

ⓐ ⓑ ⓒ ⓓ

(iv) An onto homomorphism is called

(a) epimorphism (b) monomorphism

(c) isomorphism (d) none of these

ⓐ ⓑ ⓒ ⓓ

(v) A one-one homomorphism is called

(a) epimorphism (b) monomorphism

(c) isomorphism (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vi) A bijective homomorphism is called

(a) epimorphism (b) monomorphism

(c) isomorphism (d) none of these

ⓐ ⓑ ⓒ ⓓ

(vii) A homomorphism from a group G to itself is called _____ of G.

(a) endomorphism (b) automorphism

(c) kernel of homomorphism (d) none of these

ⓐ ⓑ ⓒ ⓓ

(viii) An isomorphism from a group G to itself is called _____ automorphism of G.
(a) endomorphism (b) automorphism
(c) kernel of homomorphism (d) none of these
ⓐ ⓑ ⓒ ⓓ

(ix) The homomorphic image of a cyclic group is
(a) not cyclic (b) non-abelian
(c) cyclic (d) none of these
ⓐ ⓑ ⓒ ⓓ

(x) Every group of prime order is
(a) not cyclic (b) non-abelian
(c) cyclic (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xi) The homomorphic image of a cyclic group is
(a) not cyclic (b) non-abelian
(c) abelian (d) none of these
ⓐ ⓑ ⓒ ⓓ

(xii) Every group of prime order is
(a) not cyclic (b) non-abelian
(c) abelian (d) none of these
ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.2 Solve / answer the following short questions:

(i) Define an involution.

(ii) Define homomorphism.

(iii) Define -
(a) epimorphism **(b)** monomorphism
(c) isomorphism

(iv) Let $(R,+)$ be the group of all real numbers and $(R',\cdot)$ be the group of nonzero real numbers. Define $\phi: R \to R'$ by $\phi(x) = 3^x$. Show that ϕ is a homomorphism from R into R'.

(v) Let G be the group of integers under addition. For the integer $x \in G$, define ϕ by $\phi(x) = 3x$. Show that $\phi: G \to G$ is a homomorphism.

(vi) Let G be any abelian group, and $\phi: G \to G$ is defined by $\phi(x) = x^3$ for all $x \in G$. Show that ϕ is a homomorphism.

(vii) Let G be any abelian group, and $\phi: G \to G$ is defined by $\phi(x) = x^n$ for all $x \in G$, where n is an integer. Show that ϕ is a homomorphism.

(viii) Show that the mapping $\phi: G \to G$ defined by $\phi(x) = e$ for all $x \in G$, where e is an identity element of G, is a homomorphism.

(ix) Show that the mapping $\phi: G \to G$ defined by $\phi(x) = x$ for all $x \in G$ is a homomorphism.

(x) Let G be the group of integers under addition. For the integer $x \in G$ define ϕ by $\phi(x) = 2x$. Show that $\phi: G \to G$ is a homomorphism.

(xi) If $\phi: G \to G'$ is a homomorphism of G into G' and e is an identity element of G, then show that $\phi(e)$ is an identity element of G'.

(xii) Let $\phi: G \to G'$ be an onto homomorphism and H' be a subgroup of G'. Show that $\phi^{-1}(H')$ is a subgroup of G.

Long Questions

Q.3 Let $(R^+, \cdot)$ and $(R, +)$ be two groups. Define $\phi: R^+ \to R$ by $\phi(x) = \ln x^2$. Show that ϕ is an isomorphism.

Q.4 Let G be any group, g a fixed element in G. Define $\phi: G \to G$ by $\phi(x) = g^{-1}xg$ for all $x \in G$. Prove that ϕ is an isomorphism.

SUMMARY

- An element of order 2 in a group G is called an involution.
- A group of even order contains at least one involution.
- A mapping ϕ from a group G into a group G' is said to be a homomorphism if for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.
- An onto homomorphism is called an epimorphism.
- A one-one homomorphism is called a monomorphism.
- A bijective homomorphism is called an isomorphism.
- Two groups G and G' are said to be isomorphic if there is an isomorphism $\phi: G \to G'$. In this case we write $G \approx G'$.
- A homomorphism from a group G to itself is called an endomorphism of G.
- An isomorphism from a group G to itself is called an automorphism of G.
- The kernel of homomorphism $\phi: G \to G'$ is the set of those elements of G whose image is the identity element of G'.
- A homomorphism $\phi: G \to G'$ is one-one if and only if $Ker\phi = \{e\}$.

- The homomorphic image of a group is itself a group.
- If $\phi : G \to G'$ is a homomorphism of a group G onto another group G', then $|\phi(a)| = |a|$ for $a \in G$.
- The homomorphic image of a cyclic group is cyclic.
- Any two cyclic groups of the same order are isomorphic.
- Any two infinite cyclic groups are isomorphic.
- If $\phi : G \to G'$ is an onto homomorphism and H is a subgroup of G, then $\phi(H)$ is a subgroup of G'.
- If $\phi : G \to G'$ is an onto homomorphism and H' is a subgroup of G', then $\phi^{-1}(H')$ is a subgroup of G.
- By embedding G into G', we mean that there is a subgroup of G' which is isomorphic to G.
- Every group is isomorphic to a subgroup of a symmetric group.
- Every group is isomorphic to some permutation group.
- Any group G can be embedded in a group of bijective mappings of a certain set.
- If $G = < a : a^n = e >$ is a cyclic group, then a^m is a generator of G if and only if n and m are relatively prime.
- Every group of prime order is cyclic.
- Every group of prime order is abelian.
- A non-commutative group has at least six elements.

*****

Chapter 6

COMPLEXES IN GROUPS

In this chapter, we shall discuss complexes in groups, centre of a group, normalizer and centralizer in groups. Some results about these topics are also proved.

6-1 Complexes in Groups

6-1.1 Definition: An arbitrary subset X of a group G is said to be a *complex* in G.

For example, the subsets

$$X = \{ab, a^2b\} \text{ and } Y = \{e, b, ab\}$$

of a group $S_3 = \{e, a, a^2, b, ab, a^2b\}$ are two complexes in S_3.

6-1.2 Definition: Two complexes X and Y in a group G are said to be *permutable* if $XY = YX$, i.e. for some $x \in X$ and $y \in Y$, there exist some $x' \in X$ and $y' \in Y$ such that $xy = y'x'$.

Note: Every two complexes X and Y in an abelian group G are permutable.

6-1.3 Theorem: *A nonempty complex H of a group G is a subgroup of G if and only if $HH^{-1} \subseteq H$.*

Proof: Let H be a subgroup of G. Let $x \in HH^{-1}$, then there exist $h_1, h_2 \in H$ such that

$$x = h_1 h_2^{-1}$$

Since H is a subgroup of G, so $h_1, h_2 \in H$

$$\Rightarrow h_1 h_2^{-1} \in H$$
$$\Rightarrow x \in H$$
$$\Rightarrow HH^{-1} \subseteq H$$

Conversely, let $HH^{-1} \subseteq H$, then we have to show that H is a subgroup of G, for this let $a, b \in H$. Since $b \in H$, so $b^{-1} \in H^{-1}$.

Now

$$a \in H, b^{-1} \in H^{-1}$$
$$\Rightarrow ab^{-1} \in HH^{-1}$$
$$\Rightarrow ab^{-1} \in H \qquad \because HH^{-1} \subseteq H$$

This shows that H is a subgroup of G.

Note: A subgroup is a complex but a complex need not be a subgroup.

6-1.4 Theorem: *If H, K are subgroups of a G, then HK is a subgroup of G if and only if H and K are permutable, i.e. $HK = KH$.*

PU, 2011; 2003; 2001; 1985; 1983 (M.Sc. Math)

Proof: Let HK be a subgroup of G, then we have to show that $HK = KH$. For this let $x \in HK$, then

$$x = hk \text{ for some } h \in H, k \in K$$

Since KH is a subgroup of G, so

$$x \in HK$$
$$\Rightarrow x^{-1} \in HK$$
$$\Rightarrow (hk)^{-1} \in HK \qquad \because x = hk$$
$$\Rightarrow k^{-1}h^{-1} \in HK \qquad \because (hk)^{-1} = k^{-1}h^{-1}$$

Since H and K are subgroups of G, so

$$h \in H, k \in K$$
$$\Rightarrow h^{-1} \in H, k^{-1} \in K$$
$$\Rightarrow k^{-1}h^{-1} \in KH$$
$$\Rightarrow HK \subseteq KH \qquad \ldots(1)$$

Conversely, let $x \in KH$, then

$$x = kh \text{ for some } h \in H, k \in K$$

Now

$$x^{-1} = (kh)^{-1}$$
$$= h^{-1}k^{-1} \in HK \qquad \because h^{-1} \in H, k^{-1} \in K$$

Since HK is a subgroup of G, so $x^{-1} \in HK$

$$\Rightarrow x \in HK$$
$$\Rightarrow KH \subseteq HK$$

Combining (1) and (2), we have ...(2)

$$HK = KH$$

Conversely, if $HK = KH$, then we have to show that HK is a subgroup of G. For this let $x, y \in HK$, then there are $h_1, h_2 \in H, k_1, k_2 \in K$ such that

$$x = h_1k_1,\ y = h_2k_2$$

Next consider

$$\begin{aligned} xy^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= (h_1k_1)(k_2^{-1}h_2^{-1}) \\ &= h_1(k_1k_2^{-1})h_2^{-1} \\ &= h_1k_3h_2^{-1} && (k_3 = k_1k_2^{-1}) \\ &= h_1h_2^{-1}k_3 && \because HK = KH \\ &= h_3k_3 && (h_3 = h_1h_2^{-1}) \end{aligned}$$

Since H and K are subgroups of G, so

$$h_1, h_2 \in H$$
$$\Rightarrow h_3 = h_1h_2^{-1} \in H$$

and

$$k_1, k_2 \in K$$
$$\Rightarrow k_3 = k_1k_2^{-1} \in K$$
$$\Rightarrow h_3k_3 \in HK$$
$$\Rightarrow xy^{-1} \in HK$$

This show sthat HK is a subgroup of G.

6-2 Centre of a Group

6-2.1 Definition:

The *centre* of a group G is denoted by $Z(G)$ and defined as

$$Z(G) = \{z \in G : zx = xz \text{ for all } x \in G\}$$

If e is the identity element of a group G, then

$$ex = xe, \quad \forall x \in G$$

Therefore, $e \in Z(G)$, so the centre of a group is always a nonempty set.

6-2.2 Example: *Find the centre of* $V_4 = \{e, a, b, ab\}$.

Solution: Consider e and operate it with every element of V_4

$$e.e = e = e.e \qquad e.b = b = b.e$$
$$e.a = a = a.e \qquad e.(ab) = ab = (ab).e$$

This shows that e commutes with every element of V_4, so

$$e \in Z(V_4)$$

Consider a and operate it with every element of V_4

$$a.e = a = e.a \quad | \quad a.b = ab = b.a$$
$$a.a = e = a.a \quad | \quad a.(ab) = b = (ab).a$$

This shows that a commutes with every element of V_4, so

$$a \in Z(V_4)$$

Consider b and operate it with every element of V_4

$$b.e = b = e.b \quad | \quad b.b = e = b.b$$
$$b.a = ab = a.b \quad | \quad b.(ab) = a = (ab).b$$

This shows that b commutes with every element of V_4, so

$$b \in Z(V_4)$$

Consider ab and operate it with every element of V_4

$$(ab).e = ab = e.(ab) \quad | \quad (ab).b = a = b.(ab)$$
$$(ab).a = b = a.(ab) \quad | \quad (ab).(ab) = e = (ab).(ab)$$

This shows that ab commutes with every element of V_4, so

$$ab \in Z(V_4)$$

This shows that

$$Z(V_4) = \{e, a, b, ab\} = V_4$$

6-2.3 Example: *Show that centre of an abelian group is the group itself.*
Solution: Let G be an abelian group.
Let $x \in G$, then, since G is abelian, so

$$xg = gx, \qquad \forall g \in G$$

This shows that $x \in Z(G)$, so

$$G \subseteq Z(G)$$

But, by definition, $Z(G)$ consists of elements of G, i.e.

$$Z(G) \subseteq G$$

Combining these, we have

$$Z(G) = G$$

6-2.4 Example:

Find the centre of $S_3 = \{e, a, a^2, b, ab, a^2b\}$.

Solution: Consider

PU, 2008 (M.Sc. Math)

$$e \cdot e = e,\ e \cdot a = a,\ e \cdot a^2 = a^2,\ e \cdot b = b,\ e \cdot (ab) = ab,\ e \cdot (a^2b) = a^2b$$
$$e \cdot e = e,\ a \cdot e = a,\ a^2 \cdot e = a^2,\ b \cdot e = b,\ (ab) \cdot e = ab,\ (a^2b) \cdot e = a^2b$$
$$\Rightarrow e \in S_3$$

$$a\cdot(ab)=a^2b, \qquad (ab)\cdot a=b$$
$$\Rightarrow a\cdot(ab)\neq(ab)\cdot a$$
$$\Rightarrow a,(ab)\notin S_3$$
$$a^2\cdot b=a^2b, \qquad b\cdot a^2=ab$$
$$\Rightarrow a^2\cdot b\neq b\cdot a^2$$
$$\Rightarrow a^2,b\notin S_3$$
$$(a^2b)\cdot b=a^2, \qquad b\cdot(a^2b)=a$$
$$\Rightarrow (a^2b)\cdot b\neq b\cdot(a^2b)$$
$$\Rightarrow a^2b\notin S_3$$

This shows that $Z(S_3)=\{e\}$.

6-2.5 Theorem: *Centre $Z(G)$ of a group G is an abelian subgroup of G.*

PU, 2008 (M.Sc. Math)

Proof: Let $a,b\in Z(G)$, then by definition of centre of group

$$ax=xa \quad \text{and} \quad bx=xb, \ \forall\ x\in G$$

Now

$$bx=xb$$
$$\Rightarrow b^{-1}(bx)b^{-1}=b^{-1}(xb)b^{-1}$$
$$\Rightarrow (b^{-1}b)xb^{-1}=b^{-1}x(bb^{-1})$$
$$\Rightarrow exb^{-1}=b^{-1}xe \qquad \because b^{-1}b=e=bb^{-1}$$
$$\Rightarrow xb^{-1}=b^{-1}x, \ \forall\ x\in G$$

Next consider

$$(ab^{-1})x=a(b^{-1}x) \qquad \text{(using associative law)}$$
$$=a(xb^{-1}) \qquad \because b^{-1}x=xb^{-1}$$
$$=(ax)b^{-1} \qquad \text{(using associative law)}$$
$$=(xa)b^{-1} \qquad \because ax=xa$$
$$=x(ab^{-1}) \qquad \text{(using associative law)}$$
$$\Rightarrow ab^{-1}\in Z(G)$$

This shows that $Z(G)$ is a subgroup of G.

Next we show that $Z(G)$ is abelian. For any $a,b\in Z(G)$, $a,b\in G$, because $Z(G)$ is a subgroup of G.

Now $b\in G$ and $a\in G$, then using the definition of centre, we have

$$ab=ba$$

This shows that $Z(G)$ is an abelian subgroup of G.

This completes the proof.

6-3 Normalizer in a Group

6-3.1 Definition: Let G be a group and $a \in G$. The *normalizer* or *centralizer* of a in G is defined as

$$N(a) = \{x \in G : xa = ax\}$$

6-3.2 Theorem:
Let G be a group and $a \in G$, then $N(a) = \{x \in G : xa = ax\}$ is a subgroup of G.

Proof: Let $x, y \in N(a)$, then $xa = ax$ and $ya = ay$.

Now
$$ya = ay$$
$$\Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$$
$$\Rightarrow eay^{-1} = y^{-1}ae$$
$$\Rightarrow ay^{-1} = y^{-1}a$$

Next consider

$$\begin{aligned}(xy^{-1})a &= x(y^{-1}a) && \text{(using associative law)}\\ &= x(ay^{-1}) && \because y^{-1}a = ay^{-1}\\ &= (xa)y^{-1} && \text{(using associative law)}\\ &= (ax)y^{-1} && \because xa = ax\\ &= a(xy^{-1}) && \text{(using associative law)}\end{aligned}$$

$$\Rightarrow xy^{-1} \in N(a)$$

This shows that $N(a)$ is a subgroup of G.

6-3.3 Definition: Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with X is called *normalizer* of X in G and is denoted by $N_G(X)$.

In other words

$$N_G(X) = \{a \in G : aX = Xa\}$$

Note: Since $eX = X = Xe$, so $e \in N_G(X)$, i.e. $N_G(X)$ is always nonempty.

Note: If G is an abelian group, then $aX = Xa$ for all $a \in G$, so every element of G is in $N_G(X)$, i.e. $N_G(X) = G$.

6-3.4 Example:
If $V_4 = \{e, a, b, ab\}$ and $H = \{e, a\}$, then find $N_{V_4}(H)$.

Solution: The convenient way finding the nrmalizer of H in V_4 is to write Cayley table of $V_4 = \{e, a, b, ab\}$, so first we write Cayley table as we discussed in chapter 4.

•	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Cayley Table of V_4

Next, using above table, we find those elements of V_4 which permute with H as follows:

$$eH = e\{e,a\} = \{ee, ea\} = \{e,a\}$$
$$He = \{e,a\}e = \{ee, ae\} = \{e,a\}$$
$$\Rightarrow eH = He$$
$$\Rightarrow e \in N_{V_4}(H)$$
$$aH = a\{e,a\} = \{ae, a^2\} = \{a,e\} \qquad \because a^2 = e$$
$$Ha = \{e,a\}a = \{ea, a^2\} = \{a,e\} \qquad \because a^2 = e$$
$$\Rightarrow aH = Ha$$
$$\Rightarrow a \in N_{V_4}(H)$$
$$bH = b\{e,a\} = \{be, ba\} = \{b, ab\} \qquad \because ba = ab$$
$$Hb = \{e,a\}b = \{eb, ab\}$$
$$\Rightarrow bH = Hb$$
$$\Rightarrow b \in N_{V_4}(H)$$
$$abH = ab\{e,a\} = \{abe, ab.a\} = \{ab, b\} \quad \because ab.a = b$$
$$Hab = \{e,a\}ab = \{eab, a.ab\} = \{ab, b\} \quad \because a.ab = b$$
$$\Rightarrow abH = Hab$$
$$\Rightarrow ab \in N_{V_4}(H)$$
$$\Rightarrow N_{V_4}(H) = \{e,a,b,ab\} = V_4$$

6-3.5 Example: *If $V_4 = \{e,a,b,ab\}$ and $X = \{a,b\}$, then find the normalizer of X in V_4.*

Solution: Let us consider

$eX = \{a,b\}$	$Xe = \{a,b\}$
$aX = \{e,ab\}$	$Xa = \{e,ab\}$
$bX = \{ab,e\}$	$Xb = \{ab,e\}$
$abX = \{b,a\}$	$Xab = \{b,a\}$

This shows that every element of V_4 permutes with X, so each element of V_4 is in $N_{V_4}(X)$, i.e. $N_{V_4}(X) = V_4$.

Note: Since V_4 is an abelian group, so normalizer of any complex in V_4 is the group V_4 itself.

6-3.6 Example:

If $G =< a,b : a^3 = b^2 = (ab)^2 = e >$ *and* $H = \{e,b\}, K = \{e,a,a^2\}$.

Find $N_G(H)$ *and* $N_G(K)$.

PU, 2013 (M.Sc. Math)

Solution: We know that

$$G =< a,b : a^3 = b^2 = (ab)^2 = e >$$

is a symmetry group of an equilateral triangle, so

$$G = \{ e, a, a^2, b, ab, a^2b \} = S_3$$

Cayley table of S_3, discussed in chapter 4, is given below:

•	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Cayley Table of S_3

Next, using above table, we find those elements of S_3 which permute with H as follows:

$$eH = e\{e,b\} = \{ee,eb\} = \{e,b\}$$

$$He = \{e,b\}e = \{ee,be\} = \{e,b\}$$

$$\Rightarrow eH = He$$

$$\Rightarrow e \in N_{S_3}(H)$$

$$aH = a\{e,b\} = \{ae,ab\} = \{a,ab\}$$

$$Ha = \{e,b\}a = \{ea,ba\} = \{a,a^2b\} \qquad \because ba = a^2b$$

$$\Rightarrow aH \neq Ha$$

$$\Rightarrow a \notin N_{S_3}(H)$$

$$a^2H = a^2\{e,b\} = \{a^2e,a^2b\} = \{a^2,a^2b\}$$

$$Ha^2 = \{e,b\}a^2 = \{ea^2,ba^2\} = \{a^2,ab\} \qquad \because ba^2 = ab$$

$$\Rightarrow a^2H \neq Ha^2$$

$$\Rightarrow a^2 \notin N_{S_3}(H)$$

$$bH = b\{e,b\} = \{be,b.b\} = \{b,e\} \qquad \because b.b = e$$

$$Hb = \{e,b\}b = \{eb,b.b\} = \{b,e\} \qquad \because b.b = e$$

$\Rightarrow bH = Hb$

$\Rightarrow b \in N_{S_3}(H)$

$abH = ab\{e,b\} = \{abe, ab.b\} = \{ab, a\} \quad \because ab.b = a$

$Hab = \{e,b\}ab = \{eab, b.ab\} = \{ab, a^2b\} \quad \because b.ab = a^2b$

$\Rightarrow abH \neq Hab$

$\Rightarrow ab \notin N_{S_3}(H)$

$a^2bH = a^2b\{e,b\} = \{a^2be, a^2b.b\} = \{a^2b, a^2\} \quad \because a^2b.b = a^2$

$Ha^2b = \{e,b\}a^2b = \{ea^2b, b.a^2b\} = \{a^2b, a\} \quad \because b.a^2b = a$

$\Rightarrow a^2bH \neq Ha^2b$

$\Rightarrow a^2b \notin N_{S_3}(H)$

This shows that $N_G(H) = N_{S_3}(H) = \{e,b\}$

Next, we find those elements of S_3 which permute with K as follows:

$eK = e\{e,a,a^2\} = \{ee, ea, ea^2\} = \{e,a,a^2\}$

$Ke = \{e,a,a^2\}e = \{ee, ae, a^2e\} = \{e,a,a^2\}$

$\Rightarrow eK = Ke$

$\Rightarrow e \in N_{S_3}(K)$

$aK = a\{e,a,a^2\} = \{ae, aa, aa^2\} = \{a,a^2,e\} \quad \because aa^2 = e$

$Ka = \{e,a,a^2\}a = \{ea, aa, a^2a\} = \{a,a^2,e\} \quad \because a^2a = e$

$\Rightarrow aK = Ka$

$\Rightarrow a \in N_{S_3}(K)$

$a^2K = a^2\{e,a,a^2\} = \{a^2e, a^2a, a^2a^2\} = \{a^2,e,a\}$

$Ka^2 = \{e,a,a^2\}a^2 = \{ea^2, aa^2, a^2a^2\} = \{a^2,e,a\}$

$\Rightarrow a^2K = Ka^2$

$\Rightarrow a^2 \in N_{S_3}(K)$

$bK = b\{e,a,a^2\} = \{be, ba, ba^2\} = \{b, a^2b, ab\}$

$Kb = \{e,a,a^2\}b = \{eb, ab, a^2b\} = \{b, ab, a^2b\}$

$\Rightarrow bK = Kb$

$\Rightarrow b \in N_{S_3}(K)$

$abK = ab\{e,a,a^2\} = \{abe, ab.a, ab.a^2\} = \{ab, b, a^2b\}$

$Kab = \{e,a,a^2\}ab = \{eab, a.ab, a^2.ab\} = \{ab, a^2b, b\}$

$\Rightarrow abK = Kab$

$\Rightarrow ab \in N_{S_3}(K)$

$$a^2bK = a^2b\{e,a,a^2\} = \{a^2be, a^2b.a, a^2b.a^2\} = \{a^2b, ab, b\}$$

$$Ka^2b = \{e,a,a^2\}a^2b = \{ea^2b, a.a^2b, a^2.a^2b\} = \{a^2b, b, ab\}$$

$$\Rightarrow a^2bK = Ka^2b$$

$$\Rightarrow a^2b \in N_{S_3}(K)$$

This shows that

$$N_G(K) = N_{S_3}(K)$$

$$= \{e,a,a^2,b,ab,a^2b\} = G$$

6-3.7 Example: *If* $S_3 = \{e,a,a^2,b,ab,a^2b\}$ *and* $X = \{a,b\}$, *then find the normalizer of* X *in* S_3.

Solution: Let us consider

$eX = \{a,b\}$	$Xe = \{a,b\}$
$aX = \{a^2,ab\}$	$Xa = \{a^2,a^2b\}$
$a^2X = \{e,a^2b\}$	$Xa^2 = \{e,ab\}$
$bX = \{a^2b,e\}$	$Xb = \{ab,e\}$
$abX = \{b,a\}$	$Xab = \{a^2b,a^2\}$
$a^2bX = \{ab,a^2\}$	$Xa^2b = \{b,a\}$

Since only e permutes with X, so

$$N_{S_3}(X) = \{e\}$$

6-3.8 Example: *If* $S_3 = \{e,a,a^2,b,ab,a^2b\}$ *and* $X = \{ab,a^2b\}$, *then find the normalizer of* X *in* S_3.

Solution: Let us consider

$$eX = e\{ab,a^2b\} = \{eab, ea^2b\} = \{ab,a^2b\}$$

$$Xe = \{ab,a^2b\}e = \{abe,a^2be\} = \{ab,a^2b\}$$

$$\Rightarrow eX = Xe$$

$$\Rightarrow e \in N_{S_3}(X)$$

$$aX = a\{ab,a^2b\} = \{a.ab, a.a^2b\} = \{a^2b,b\}$$

$$Xa = \{ab,a^2b\}a = \{ab.a, a^2b.a\} = \{b,ab\}$$

$$\Rightarrow aX \neq Xa$$

$$\Rightarrow a \notin N_{S_3}(X)$$

$$a^2X = a^2\{ab,a^2b\} = \{a^2.ab, a^2.a^2b\} = \{b,ab\}$$

$$Xa^2 = \{ab,a^2b\}a^2 = \{ab.a^2, a^2b.a^2\} = \{a^2b,b\}$$

$$\Rightarrow a^2X \neq Xa^2$$

$\Rightarrow a^2 \notin N_{S_3}(X)$

$bX = b\{ab, a^2b\} = \{b.ab, b.a^2b\} = \{a^2, a\}$

$Xb = \{ab, a^2b\}b = \{ab.b, a^2b.b\} = \{a, a^2\}$

$\Rightarrow bX = Xb$

$\Rightarrow b \in N_{S_3}(X)$

$abX = ab\{ab, a^2b\} = \{ab.ab, ab.a^2b\} = \{e, a^2\}$

$Xab = \{ab, a^2b\}ab = \{ab.ab, a^2b.ab\} = \{e, a\}$

$\Rightarrow abX \neq Xab$

$\Rightarrow ab \notin N_{S_3}(X)$

$a^2bX = a^2b\{ab, a^2b\} = \{a^2b.ab, a^2b.a^2b\} = \{a, e\}$

$Xa^2b = \{ab, a^2b\}a^2b = \{ab.a^2b, a^2b.a^2b\} = \{a^2, e\}$

$\Rightarrow a^2bX \neq Xa^2b$

$\Rightarrow a^2b \notin N_{S_3}(X)$

$\Rightarrow N_{S_3}(X) = \{e, b\}$

6-3.9 Example: *If and* $X = \{a, b\}$, *then find* $N_{D_4}(X)$.

Solution: We know that

$$D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

With Cayley table given below

$\cdot$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Cayley Table of D_4

Using above table, we have

$eX = e\{a, b\} = \{a, b\}$

$aX = a\{a, b\} = \{a^2, ab\}$

$a^2X = a^2\{a, b\} = \{a^3, a^2b\}$

$a^3X = a^3\{a, b\} = \{e, a^3b\}$

$Xe = \{a, b\}e = \{a, b\}$

$Xa = \{a, b\}a = \{a^2, a^3b\}$

$Xa^2 = \{a, b\}a^2 = \{a^3, a^2b\}$

$Xa^3 = \{a, b\}a^3 = \{e, ab\}$

$$bX = b\{a,b\} = \{a^3, e\} \qquad Xb = \{a,b\}b = \{ab, e\}$$
$$abX = ab\{a,b\} = \{b,a\} \qquad Xab = \{a,b\}ab = \{a^2b, a^3\}$$
$$a^2bX = a^2b\{a,b\} = \{ab, a^2\} \qquad Xa^2b = \{a,b\}a^2b = \{a^3b, a^2\}$$
$$a^3bX = a^3b\{a,b\} = \{a^2b, a^3\} \qquad Xa^3b = \{a,b\}a^3b = \{b,a\}$$

We note that only

$$eX = Xe$$
$$a^2X = Xa^2$$

Therefore, only e and a^2 are in $N_{D_4}(X)$, so

$$N_{D_4}(X) = \{e, a^2\}$$

6-4 Centralizer in a Group

6-4.1 Definition: Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with the elements of X is called *centralizer* of X in G and is denoted by $C_G(X)$.

In other words

$$C_G(X) = \{a \in G : ax = xa,\ x \in X\}$$

Note: Since $ex = x = xe$ for all $x \in X$, so $e \in C_G(X)$, i.e. $C_G(X)$ is always nonempty.

Note: If G is an abelian group, then $ax = xa$ for all $a \in G$, $x \in X$, so every element of G is in $C_G(X)$, i.e. $C_G(X) = G$.

6-4.2 Example: *If* $V_4 = \{e,a,b,ab\}$ *and* $X = \{a,b\}$, *then find the centralizer of* X *in* V_4.

Solution: Let us consider

$$e.e = e = e.e \qquad e.b = b = b.e$$
$$e.a = a = a.e \qquad e.(ab) = ab = (ab).e$$
$$a.e = a = e.a \qquad a.b = ab = b.a$$
$$a.a = e = a.a \qquad a.(ab) = b = (ab).a$$
$$b.e = b = e.b \qquad b.b = e = b.b$$
$$b.a = ab = a.b \qquad b.(ab) = a = (ab).b$$
$$(ab).e = ab = e.(ab) \qquad (ab).b = a = b.(ab)$$
$$(ab).a = b = a.(ab) \qquad (ab).(ab) = e = (ab).(ab)$$

This shows that each element of V_4 permutes with the elements of X, so $C_{V_4}(X) = V_4$.

6-4.3 Example: *If* $X = \{a,b\}$, *then find* $C_{S_3}(X)$.

Solution: We know that

$$S_3 = \{e, a, a^2, b, ab, a^2b\}$$

Using Cayley table of S_3, we find those elements of S_3, which permute with the elements of X as follows:

$$e.a = a = a.e$$

$$e.b = b = b.e$$

This shows that e permutes with both elements a and b of X, so

$$e \in C_{S_3}(X)$$

Since

$$a.b = ab$$

$$b.a = a^2b$$

This shows that a does not permute with the element b of X and b also does not permute with the element a of X, so

$$a, b \notin C_{S_3}(X)$$

Now, $b.a^2 = ab \neq a^2.b$, so $a^2 \notin C_{S_3}(X)$.

Similarly, $ab.b \neq b.ab \Rightarrow ab \notin C_{S_3}(X)$

and, $a^2b.a \neq a.a^2b \Rightarrow a^2b \notin C_{S_3}(X)$

Thus, $C_{S_3}(X) = \{e\}$

6-5 Conjugacy Classes in a Group

6-5.1 Definition:

If $a,b \in G$, then b is said to be a *conjugate* of a in G if there exists an element $g \in G$ such that $b = g^{-1}ag$.

Symbolically, we write $a \sim b$ and refer to this relation as *conjugacy*.

Note: We can also define the conjugate of an element as follows:

If $a,b \in G$, then b is said to be a *conjugate* of a in G if there exists an element $g \in G$ such that $b = gag^{-1}$.

6-5.2 Theorem: *Conjugacy between elements of a group is an equivalence relation on G.*

PU, 2009 (M.Sc. Math)

Proof: Let $a,b,c \in G$.

1. **Reflexive**

Since $a = e^{-1}ae$, so a is conjugate of a in G, i.e. $a \sim a$.

This shows that ~ is reflexive.

2. Symmetric

Let $a \sim b$, then there is $x \in G$ such that

$$b = x^{-1}ax$$
$$\Rightarrow xbx^{-1} = x(x^{-1}ax)x^{-1}$$
$$\Rightarrow (x^{-1})^{-1}b(x^{-1}) = eae$$
$$\Rightarrow y^{-1}by = a \qquad \because y = x^{-1} \in G$$
$$\Rightarrow b \sim a$$

This shows that ~ symmetric.

3. Transitive

Let $a \sim b$, $b \sim c$, then there are $x, y \in G$ such that

$$b = x^{-1}ax \qquad ...(1)$$

and $$c = y^{-1}by \qquad ...(2)$$

Using the value of b from (1) in (2), we have

$$c = y^{-1}(x^{-1}ax)y$$
$$= (y^{-1}x^{-1})a(xy)$$
$$= (xy)^{-1}a(xy)$$
$$\Rightarrow a \sim c \qquad \because xy \in G$$

This shows that ~ is transitive.

Hence ~ is an equivalence relation.

6-5.3 Definition: If b is a conjugate of a, then we say that a and b are *conjugate elements.*

6-5.4 Definition: The set of all those elements of a group G which are conjugate of a in G is called *conjugate class of a in G*. It is denoted by $C(a)$ or C_a.

Thus,

$$C(a) = \{x \in G : a \sim x\}$$

Or

$$C(a) = \{g^{-1}ag : g \in G\}$$

6-5.5 Theorem:

Conjugate elements have same order.

Proof: Let G be a group and a and b the conjuagate elements.

Let $|a| = m$, $|b| = n$, then $a^m = e$, $b^n = e$.

Since a and b the conjuagate elements, so there is some $g \in G$ such that

$$a = g^{-1}bg$$
$$\Rightarrow a^n = (g^{-1}bg)^n$$

$$\Rightarrow a^n = g^{-1}b^n g$$
$$= g^{-1}eg \qquad \because b^n = e$$
$$= g^{-1}g$$
$$= e$$
$$\Rightarrow m \le n \qquad (1) \qquad \because |a| = m$$
$$a^m = (g^{-1}bg)^m$$
$$e = g^{-1}b^m g \qquad \because a^m = e$$
$$geg^{-1} = b^m$$
$$e = b^m$$
$$\Rightarrow n \le m \qquad (2) \qquad \because |b| = n$$

From (1) and (2), we have

$$m = n$$

This shows that conjugate elements have same order.

6-5.6 Definition: An element a of a group G is said to be *self conjugate* if there exists an element $g \in G$ such that $a = g^{-1}ag$.

Identity element e is self conjugate.

Every element of an abelian group is self conjugate.

6-5.7 Definition: If G is a group and $x, y \in G$, $x^{-1}y^{-1}xy$ is called the *commutator* of x and y or, more briefly, a *commutator*. We often write $[x, y]$ for the commutator $x^{-1}y^{-1}xy$.

6-5.8 Example: *Prove that the inverse of a commutator is a commutator.*
Solution: Let G be a group and $x, y \in G$. If z is the commutator of x and y, then

$$z = [x, y] = x^{-1}y^{-1}xy$$

Taking inverse, we have

$$z^{-1} = (x^{-1}y^{-1}xy)^{-1}$$
$$= y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1}$$
$$= y^{-1}x^{-1}yx$$
$$= [y, x]$$

6-5.9 Example: *For $V_4 = \{e, a, b, ab\}$, find the conjugate classes*
(i) $C(e)$ (ii) $C(a)$ (iii) $C(b)$ (iv) $C(ab)$

Solution: $V_4 = \{e, a, b, ab\}$

(i) To find $C(e)$, we have to find those elements of V_4 which are conjugate of e. For this we check all the elements of V_4 turn by turn as follows:

$$e \cdot e \cdot e^{-1} = e$$
$$a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$
$$b \cdot e \cdot b^{-1} = b \cdot b^{-1} = e$$
$$ab \cdot e \cdot (ab)^{-1} = ab \cdot (ab)^{-1} = e$$

This shows that only e is conjugate of e, so $C(e) = \{e\}$.

(ii) To find $C(a)$, we have to find those elements of V_4 which are conjugate of a. For this we check all the elements of V_4 turn by turn as follows:

$$e \cdot a \cdot e^{-1} = a$$
$$a \cdot a \cdot a^{-1} = a \cdot a \cdot a = a$$
$$b \cdot a \cdot b^{-1} = ab \cdot b = a$$
$$ab \cdot a \cdot (ab)^{-1} = a \cdot ab \cdot ab = a^2 \cdot ba \cdot b = a^2 \cdot ab \cdot b = a$$

This shows that only a is conjugate of a, so $C(a) = \{a\}$.

(iii) To find $C(b)$, we have to find those elements of V_4 which are conjugate of b. For this we check all the elements of V_4 turn by turn as follows:

$$e \cdot b \cdot e^{-1} = b$$
$$a \cdot b \cdot a^{-1} = ab \cdot a = a \cdot ab = a^2 b = b$$
$$b \cdot b \cdot b^{-1} = b^2 \cdot b = b$$
$$ab \cdot b \cdot (ab)^{-1} = ab^2 \cdot ab = a \cdot e \cdot ab = a^2 b = b$$

This shows that only b is conjugate of b, so $C(b) = \{b\}$.

(iv) To find $C(ab)$, we have to find those elements of V_4 which are conjugate of ab. For this we check all the elements of V_4 turn by turn as follows:

$$e \cdot ab \cdot e^{-1} = ab$$
$$a \cdot ab \cdot a^{-1} = a^2 b \cdot a = a^2 \cdot ab = ab$$
$$b \cdot ab \cdot b^{-1} = ab \cdot b \cdot b = ab^3 = ab$$
$$ab \cdot ab \cdot (ab)^{-1} = a \cdot ab \cdot b \cdot ab = a^2 \cdot b^2 \cdot ab = e \cdot e \cdot ab = ab$$

This shows that only ab is conjugate of ab, so $C(ab) = \{ab\}$.

6-5.10 Example: *For $S_3 = \{e, a, a^2, b, ab, a^2 b\}$, find the conjugate classes*

(i) $C(e)$ (ii) $C(a)$ (iii) $C(a^2)$ (iv) $C(b)$
(v) $C(ab)$ (vi) $C(a^2b)$.

PU, 2011 (M.Sc. Math)

Solution: $S_3 = \{e, a, a^2, b, ab, a^2b\}$

First we write Cayley table of S_3 which we have discussed in chapter 4. This table will be very useful in performing operations among the elements of S_3.

$\cdot$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Cayley Table of S_3

(i) To find $C(e)$, we have to find those elements of S_3 which are conjugate of e. For this we check all the elements of S_3 turn by turn as follows:

$$e \cdot e \cdot e^{-1} = e$$
$$a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$$
$$(a^2) \cdot e \cdot (a^2)^{-1} = (a^2) \cdot (a^2)^{-1} = e$$
$$b \cdot e \cdot b^{-1} = b \cdot b^{-1} = e$$
$$ab \cdot e \cdot (ab)^{-1} = ab \cdot (ab)^{-1} = e$$
$$(a^2b) \cdot e \cdot (a^2b)^{-1} = (a^2b) \cdot (a^2b)^{-1} = e$$

This shows that only e is conjugate of e, so $C(e) = \{e\}$.

(ii) To find $C(a)$, we have to find those elements of S_3 which are conjugate of a. For this we check all the elements of S_3 turn by turn.

$$e \cdot a \cdot e^{-1} = a$$
$$a \cdot a \cdot a^{-1} = a \cdot e = a$$
$$(a^2) \cdot a \cdot (a^2)^{-1} = a^2 \cdot a \cdot a = a$$
$$b \cdot a \cdot b^{-1} = ba \cdot b = a^2b \cdot b = a^2$$
$$ab \cdot a \cdot (ab)^{-1} = ab \cdot a \cdot ab = b \cdot ab = a^2$$
$$(a^2b) \cdot a \cdot (a^2b)^{-1} = a^2b \cdot a \cdot a^2b = ab \cdot a^2b = a^2$$

This shows that only a and a^2 are conjugate of a, so

$$C(a) = \{a, a^2\}$$

(iii) To find $C(a^2)$, we have to find those elements of S_3 which are conjugate of a^2. For this we check all the elements of S_3 turn by turn.

$$e \cdot a^2 \cdot e^{-1} = a^2$$
$$a \cdot a^2 \cdot a^{-1} = e \cdot a^2 = a^2$$
$$(a^2) \cdot a^2 \cdot (a^2)^{-1} = a^2 \cdot a^2 \cdot a = a^2$$
$$b \cdot a^2 \cdot b^{-1} = b.a^2 \cdot b = ab \cdot b = a$$
$$ab \cdot a^2 \cdot (ab)^{-1} = ab \cdot a^2 \cdot ab = a^2b \cdot ab = a$$
$$(a^2b) \cdot a^2 \cdot (a^2b)^{-1} = a^2b \cdot a^2 \cdot a^2b = b \cdot a^2b = a$$

This shows that only a and a^2 are conjugate of a^2, so

$$C(a^2) = \{a, a^2\}$$

(iv) To find $C(b)$, we have to find those elements of S_3 which are conjugate of b. For this we check all the elements of S_3 turn by turn.

$$e \cdot b \cdot e^{-1} = b$$
$$a \cdot b \cdot a^{-1} = ab \cdot a^2 = a^2b$$
$$(a^2) \cdot b \cdot (a^2)^{-1} = a^2 \cdot b \cdot a = a^2b.a = ab$$
$$b \cdot b \cdot b^{-1} = b.e = b$$
$$ab \cdot b \cdot (ab)^{-1} = ab \cdot b \cdot ab = a \cdot ab = a^2b$$
$$(a^2b) \cdot b \cdot (a^2b)^{-1} = a^2b \cdot b \cdot a^2b = a^2 \cdot a^2b = ab$$

This shows that only b, ab and a^2b are conjugate of b, so

$$C(b) = \{b, ab, a^2b\}$$

(v) To find $C(ab)$, we have to find those elements of S_3 which are conjugate of ab. For this we check all the elements of S_3 turn by turn.

$$e \cdot ab \cdot e^{-1} = ab$$
$$a \cdot ab \cdot a^{-1} = a^2b \cdot a^2 = b$$
$$(a^2) \cdot ab \cdot (a^2)^{-1} = a^2 \cdot ab \cdot a = b.a = a^2b$$
$$b \cdot ab \cdot b^{-1} = ba.e = a^2b$$
$$ab \cdot ab \cdot (ab)^{-1} = ab \cdot ab \cdot ab = e \cdot ab = ab$$
$$(a^2b) \cdot ab \cdot (a^2b)^{-1} = a^2b \cdot ab \cdot a^2b = a \cdot a^2b = b$$

This shows that only b, ab and a^2b are conjugate of ab, so

$$C(ab) = \{b, ab, a^2b\}$$

(vi) To find $C(a^2b)$, we have to find those elements of S_3 which are conjugate of a^2b.

For this we check all the elements of S_3 turn by turn.

$$e \cdot a^2b \cdot e^{-1} = a^2b$$

$$a \cdot a^2b \cdot a^{-1} = b \cdot a^2 = ab$$

$$(a^2) \cdot a^2b \cdot (a^2)^{-1} = a^2 \cdot ab \cdot a = b.a = a^2b$$

$$b \cdot a^2b \cdot b^{-1} = ba^2.e = ab$$

$$ab \cdot a^2b \cdot (ab)^{-1} = ab \cdot a^2b \cdot ab = a^2 \cdot ab = b$$

$$(a^2b) \cdot a^2b \cdot (a^2b)^{-1} = a^2b \cdot a^2b \cdot a^2b = e \cdot a^2b = a^2b$$

This shows that only b, ab and a^2b are conjugate of a^2b, so

$$C(a^2b) = \{b, ab, a^2b\}$$

6-5.11 Class Equation:

Let there be r possible conjugacy classes in a finite group G of order n. Since the congugacy relation is an equivalence relation and it defines a partition of G in terms of its conjugacy classes.

Therefore, the order of group must be equal to the sum of orders of conjugacy classes, i.e.

$$|G| = |C_{a_1}| + |C_{a_2}| + |C_{a_3}| + \ldots + |C_{a_r}|$$

If $n_1, n_2, n_3, \ldots, n_r$ are the number of elements in the respective conjugacy classes, then above equation takes the form

$$n = n_1 + n_2 + n_3 + \ldots + n_r$$

or

$$n = \sum_{\alpha=1}^{r} n_\alpha$$

or

$$n = \sum_{\alpha=1}^{r} |C_{a_\alpha}|$$

This is called the *class equation* of group G.

For example, in S_3, we have

$$|S_3| = |C_e| + |C_a| + |C_b|$$

$$6 = 1 + 2 + 3$$

Note:

If G an abelian group, then every element is itself conjugate, so each

$$|C_{a_\alpha}| = 1$$

6-5.12 Theorem: *The number of elements in a conjugacy class C_a of an element a in a group G is equal to the index of its normalizer in G, i.e.*

$$|C_a| = |G : N_G(a)|$$

PU, 2012 (M.Sc. Math)

Proof: Let Ω be the collection of right cosets of normalizer $N_G(a)$ of $a \in G$. Let $N_G(a) = N$, then we have to show that the number of elements

in Ω is equal to the number of elements in C_a. For this, let us define a mapping $\phi : \Omega \to C_a$ by

$$\phi(Ng) = g^{-1}ag, \ \forall g \in G$$

(i) Well defined

First we show that ϕ is well defined, for this let

$$\begin{aligned}
& Ng_1 = Ng_2 \\
\Rightarrow\ & Ng_1g_2^{-1} = N \\
\Rightarrow\ & g_1g_2^{-1} \in N \\
\Rightarrow\ & g_1g_2^{-1} = n \quad \text{for some } n \in N \\
\Rightarrow\ & g_1 = ng_2 \\
\Rightarrow\ & g_1^{-1} = (ng_2)^{-1} \\
\Rightarrow\ & g_1^{-1}ag_1 = (ng_2)^{-1}ag_1 \\
& \qquad = g_2^{-1}n^{-1}a(ng_2) \qquad \because g_1 = ng_2 \\
& \qquad = g_2^{-1}(n^{-1}an)g_2 \\
& \qquad = g_2^{-1}ag_2 \qquad \because a \in N \therefore aN = Na \therefore n^{-1}an = a \\
\Rightarrow\ & \phi(Ng_1) = \phi(Ng_2)
\end{aligned}$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

Since for every $g^{-1}ag \in C_a$, there is some $Ng \in \Omega$ such that

$$\phi(Ng) = g^{-1}ag$$

This shows that ϕ is onto.

(iii) One-One

Next we show that ϕ is one-one, for this let

$$\begin{aligned}
& \phi(Ng_1) = \phi(Ng_2) \\
\Rightarrow\ & g_1^{-1}ag_1 = g_2^{-1}ag_2 \\
\Rightarrow\ & g_2(g_1^{-1}ag_1)g_2^{-1} = a \\
\Rightarrow\ & (g_1g_2^{-1})^{-1}a(g_1g_2^{-1}) = a \\
\Rightarrow\ & g_1g_2^{-1} \in N \\
\Rightarrow\ & Ng_1g_2^{-1} = N \\
\Rightarrow\ & Ng_1 = Ng_2
\end{aligned}$$

This shows that ϕ is one-one.

This shows that $\phi : \Omega \to C_a$ is a bijective mapping, so $|C_a| = |G : N_G(a)|$.

6-5.13 Theorem: *Let G be a finite group and $a \in G$, then the number of elements in a conjugacy class C_a of an element a in G divides the order of G, i.e. $|C_a|$ divides $|G|$.*

Proof: Since $N_G(a)$ is a subgroup of G, so by Lagrange's theorem, index of $N_G(a)$ in G divides the order of G, i.e. $|G : N_G(a)|$ divides $|G|$.

By previous theorem, we have proved that

$$|G : N_G(a)| = |C_a|$$

This shows that $|C_a|$ divides $|G|$.

6-5.14 Theorem: *The number of elements in a conjugacy class of an element in a group is finite if and only if the index of the normalizer of that element is finite.*

Proof: Let G be a group and $a \in G$, then

$$C_a = \{b \in G : b = gag^{-1} \text{ for some } g \in G\}$$

$$N_G(a) = \{g \in G : ga = ag\}$$

Since $|G : N_G(a)| = |C_a|$, so

$$|G : N_G(a)| < \infty$$

$$\Leftrightarrow |C_a| < \infty$$

Thus, the number of elements in a conjugacy class of an element in a group is finite if and only if the index of the normalizer of that element is finite.

6-5.15 Definition: Let H be a subgroup of a group G, then for $g \in G$,

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

is also a subgroup of G and is called *conjugate of H*.

In other words we say that H and gHg^{-1} are *conjugate subgroups of G*.

Thus H and K are said to be *conjugate subgroups* if

$$K = gHg^{-1} \text{ for some } g \in G$$

6-5.16 Example:

For a group $S_3 = \{e, a, a^2, b, ab, a^2b\}$, find the conjugate subgroups of $H = \{e, a, a^2\}$.

Solution: To find conjugate subgroups, we take the elements of S_3 one by one and perform the following operations with H.

$$eHe^{-1} = e\{e, a, a^2\}e^{-1} = \{eee^{-1}, eae^{-1}, ea^2e^{-1}\} = \{e, a, a^2\} = H$$

$$aHa^{-1} = a\{e, a, a^2\}a^{-1} = \{aea^{-1}, aaa^{-1}, aa^2a^{-1}\} = \{e, a, a^2\} = H$$

$$a^2H(a^2)^{-1} = a^2\{e, a, a^2\}(a^2)^{-1} = \{a^2e(a^2)^{-1}, a^2a(a^2)^{-1}, a^2a^2(a^2)^{-1}\}$$

$$= \{e, a, a^2\} = H$$

$$bHb^{-1} = b\{e,a,a^2\}b^{-1} = \{beb^{-1}, bab^{-1}, ba^2b^{-1}\} = \{e,a,a^2\} = H$$

Similarly,

$$abH(ab)^{-1} = H$$

and

$$a^2bH(a^2b)^{-1} = H$$

6-5.17 Theorem: *Two conjugate subgroups of a group G have the same order.*

Proof: Let G be a group and H and K be two conjugate, then

$$K = gHg^{-1} \text{ for some } g \in G$$

Next define a mapping $\phi : H \to K$ by

$$\phi(h) = ghg^{-1} \in K$$

(i) Well defined

First we show that ϕ is well defined, for this let

$$h_1 = h_2$$
$$\Rightarrow gh_1 = gh_2$$
$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$
$$\Rightarrow \phi(h_1) = \phi(h_2)$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

Since for every $ghg^{-1} \in K$, there is some $h \in H$ such that

$$\phi(h) = ghg^{-1}$$

This shows that ϕ is onto.

(iii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(h_1) = \phi(h_2)$$
$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$
$$\Rightarrow h_1 = h_2$$

This shows that ϕ is one-one.

This shows that $\phi : H \to K$ is a bijective mapping, so

$$|H| = |K|$$

6-5.18 Theorem: *Any two conjugate subgroups of a group G are isomorphic to each other.*

Proof: Let G be a group and H and K be two conjugate, then

$$K = gHg^{-1} \text{ for some } g \in G$$

Next define a mapping $\phi : H \to K$ by

$$\phi(h) = ghg^{-1} \in K$$

(i) Well defined

First we show that ϕ is well defined, for this let

$$h_1 = h_2$$
$$\Rightarrow gh_1 = gh_2$$
$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$
$$\Rightarrow \phi(h_1) = \phi(h_2)$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

Since for every $ghg^{-1} \in K$, there is some $h \in H$ such that

$$\phi(h) = ghg^{-1}$$

This shows that ϕ is onto.

(iii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(h_1) = \phi(h_2)$$
$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$
$$\Rightarrow h_1 = h_2$$

This shows that ϕ is one-one.

(iv) Homomorphism

Next we show that ϕ is homomorphism, for this let

$$\begin{aligned}\phi(h_1h_2) &= gh_1h_2g^{-1}\\ &= gh_1eh_2g^{-1}\\ &= gh_1g^{-1}gh_2g^{-1}\\ &= (gh_1g^{-1})(gh_2g^{-1})\\ &= \phi(h_1)\phi(h_2)\end{aligned}$$

This shows that ϕ is a homomorphism. Hence, ϕ, being bijective homomorphism, is an isomorphis. Consequently H and K are isomorphic, i.e. $H \approx K$.

6-5.19 Theorem: *The number of conjugate subgroups of a subgroup H of a group G is equal to the index of the normalizer $N_G(H)$.*

Proof: Let H be the subgroup of a group G. Let Ω be the collection of all left cosets of $N_G(H) = N$ (say) in G.

Let C_H be the collection of all conjugate subgroups of H in G, then we have to show that the number of elements in Ω is equal to the number of elements in C_H. For this, let us define a mapping $\phi : \Omega \to C_H$ by

$$\phi(gN) = gHg^{-1}, \ \forall g \in G$$

(i) Well defined

First we show that ϕ is well defined, for this let

$$g_1N = g_2N$$
$$\Rightarrow g_2^{-1}g_1N = N$$
$$\Rightarrow g_2^{-1}g_1 \in N$$
$$\Rightarrow g_2^{-1}g_1 = n \quad \text{for some } n \in N$$
$$\Rightarrow g_1 = g_2n$$
$$\Rightarrow g_1^{-1} = (g_2n)^{-1}$$
$$\Rightarrow Hg_1^{-1} = H(g_2n)^{-1}$$
$$\Rightarrow g_1Hg_1^{-1} = g_1H(n^{-1}g_2^{-1})$$
$$= g_2nH(n^{-1}g_2^{-1}) \qquad \because g_1 = g_2n$$
$$= g_2(nHn^{-1})g_2^{-1}$$
$$= g_2Hg_2^{-1} \qquad \because n \in N \therefore nH = Nn \therefore n^{-1}Hn = H$$
$$\Rightarrow \phi(g_1N) = \phi(g_2N)$$

This shows that ϕ is well defined.

(ii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(g_1N) = \phi(g_2N)$$
$$\Rightarrow g_1Hg_1^{-1} = g_2Hg_2^{-1}$$
$$\Rightarrow g_2^{-1}(g_1Hg_1^{-1})g_2 = H$$
$$\Rightarrow (g_2^{-1}g_1)H(g_1^{-1}g_2) = H$$
$$\Rightarrow (g_2^{-1}g_1)H(g_2^{-1}g_1)^{-1} = H$$
$$\Rightarrow (g_2^{-1}g_1)H = H(g_2^{-1}g_1)$$
$$\Rightarrow g_2^{-1}g_1 \in N$$
$$\Rightarrow (g_2^{-1}g_1)N = N$$
$$\Rightarrow g_1N = g_2N$$

This shows that ϕ is one-one.

(iii) Onto

Next we show that ϕ is onto.

Since for every $gHg^{-1} \in C_H$, there is some $gN \in \Omega$ such that

$$\phi(gN) = gHg^{-1}$$

This shows that ϕ is onto.

This shows that $\phi : \Omega \to C_H$ is a bijective mapping, so

$$|\Omega| = |C_H|$$

But $$|\Omega| = |G : N_G(H)|$$

Therefore $$|C_H| = |G : N_G(H)|$$

Thus, the number of conjugate subgroups of a subgroup H of a group G is equal to the index of the normalizer $N_G(H)$.

6-5.20 Definition: A group G is said to be a *p-group* if the order of every element of G can be written as p^α, for some fixed p.

For example, consider the elements of $V_4 = \{e, a, b, ab\}$ group.

Since

$$o(e) = 1 = 2^0, \qquad o(a) = 2 = 2^1,$$
$$o(b) = 2 = 2^1, \qquad o(ab) = 2 = 2^1$$

This shows that the order of every element of V_4 can be written as 2^α, for 2, so V_4 is a p-group, with $p = 2$.

6-5.21 Theorem: *The centre of a finite p-group is nontrivial.*

PU, 2012; 2010; 2009; 2002; 2000 (M.Sc. Math)

Proof: Let P be a finite p-group of order p^m. Let there be r possible conjugacy classes of P of orders $m_1, m_2, m_3, ..., m_r$ respectively.

Since the conjugacy classes define a partition of group P, so

$$p^m = m_1 + m_2 + m_3 + ... + m_r \qquad ...(1)$$

is the class equation of group P. Then each m_i divides p^m, so each m_i is of the form p^{α_i}. Therefore, (1) takes the form

$$p^m = p^{\alpha_1} + p^{\alpha_2} + p^{\alpha_3} + ... + p^{\alpha_r} \qquad ...(2)$$

Since e is self conjugate, so

$$|C_e| = 1 = p^{\alpha_1} \text{ (say)}$$

Then (2) takes the form

$$p^m = 1 + p^{\alpha_2} + p^{\alpha_3} + ... + p^{\alpha_r}$$

$$\Rightarrow 1 = p^m - (p^{\alpha_2} + p^{\alpha_3} + ... + p^{\alpha_r}) \qquad ...(3)$$

Here p divides the right hand side but does not divide the left side of (3), so let there be k classes consisting of self conjugate element. Then (2) takes the form

$$p^m = 1 + 1 + ... + 1 + p^{\alpha_{k+1}} + p^{\alpha_{k+2}} + ... + p^{\alpha_r}$$

$$p^m = k + p^{\alpha_{k+1}} + p^{\alpha_{k+2}} + ... + p^{\alpha_r}$$

$$\Rightarrow k = p^m - (p^{\alpha_{k+1}} + p^{\alpha_{k+2}} + ... + p^{\alpha_r}) \qquad ...(4)$$

Since p divides the right hand side of (4), so it must divide its left side, i.e.

p must divide k. Since $k \neq 0$ and $k \neq 1$, so $k > 2$.

This shows that there are more than one central element in P. Hence, the centre of a finite p-group is nontrivial.

This completes the proof.

6-6 Double Cosets

6-6.1 Definition: Let H, K be two subgroups of a group G and $a \in G$ be an arbitrary element of G then the set

$$HaK = \{hak : h \in H, k \in K\}$$

is called the *double coset* in G modulo (H,K) determined by a.

For example, if we consider

$$S_3 = \{e, a, a^2, b, ab, a^2b\}$$

with $H = \{e, a, a^2\}$, $K = \{e, b\}$

Then

$$\begin{aligned} HbK &= \{e, a, a^2\}b\{e, b\} \\ &= \{b, ab, a^2b\}\{e, b\} \\ &= \{b, ab, a^2b, b^2, ab^2, a^2b^2\} \\ &= \{b, ab, a^2b, e, a, a^2\} \\ &= \{e, a, a^2, b, ab, a^2b\} \end{aligned}$$

is the double coset in S_3 modulo (H,K) determined by b.

6-6.2 Theorem: *Let H, K be subgroups of a group G and $a \in G$, then the collection Ω of all double cosets HaK defines a partition of G.*

PU, 2015 (BS Math)

Proof: Let $a \in G$. then

$$a = eae \in Hak \qquad \because e \in H, e \in K$$

$$\Rightarrow a \in \bigcup_{a \in G} HaK$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} HaK \qquad \ldots(1)$$

But

$$\Rightarrow \bigcup_{a \in G} HaK \subseteq G \qquad \ldots(2)$$

Combining (1) and (2), we have

$$G = \bigcup_{a \in G} HaK \qquad \ldots(3)$$

In order to show that

$$HaK \cap HbK = \phi \text{ for all } a, b \in G, a \neq b$$

let us suppose on contrary that HaK, HbK are distinct double cosets such that

$\therefore HaK \cap HbK \neq \phi$ for some $a, b \in G, a \neq b$

Let

$$x \in HaK \cap HbK$$

$$\Rightarrow x \in HaK \text{ and } x \in HbK$$

$$\Rightarrow x = h_1 a k_1 \text{ and } x = h_2 b k_2, \qquad h_1, h_2 \in H, k_1, k_2 \in K$$

$$\Rightarrow h_1 a k_1 = x = h_2 b k_2$$

$$\Rightarrow h_1 a k_1 = h_2 b k_2$$

$$\Rightarrow a = h_1^{-1}(h_2 b k_2) k_1^{-1}$$

$$\Rightarrow a = (h_1^{-1} h_2) b (k_2 k_1^{-1}) \qquad \ldots(4)$$

Next suppose that

$$y \in HaK$$

$$\Rightarrow y = h_3 a k_3, \quad h_3 \in H, k_3 \in K$$

$$\Rightarrow y = h_3 (h_1^{-1} h_2) b (k_2 k_1^{-1}) k_3 \qquad \text{putting } a \text{ from (4)}$$

$$\Rightarrow y = (h_3 h_1^{-1} h_2) b (k_2 k_1^{-1} k_3)$$

$$\Rightarrow y = h_4 b k_4, \qquad h_3 h_1^{-1} h_2 = h_4, k_2 k_1^{-1} k_3 = k_4$$

$$\Rightarrow y \in HbK \quad \because h_4 \in H, k_4 \in K$$

$$\Rightarrow HaK \subseteq HbK \qquad \ldots(5)$$

Similarly, we can show that

$$HbK \subseteq HaK \qquad \ldots(6)$$

Combining (5) and (6), we have

$$HaK = HbK$$

This is a contradiction to our assumption that $HaK \neq HbK$.

Therefore,

$$HaK \cap HbK = \phi \text{ for all } a, b \in G, a \neq b$$

Hence, double cosets define a partition of G.

6-6.3 Theorem: *Let H, K be subgroups of a finite group G, then the complex HK contains exactly $\frac{mn}{q}$ elements, where m, n and q are orders of H, K, and $H \cap K$ respectively.*

Alternative Statement:

Let H, K be subgroups of a finite group G, then $|HK| = \frac{|H||K|}{|H \cap K|}$ *or*

$$o(HK) = \frac{o(H)o(k)}{o(H \cap K)}.$$

PU, 2000 (M.Sc. Math)

Proof: $Q = H \cap K$, being the intersection of two subgroups H and K, is a subgroup of G.

Also since H and K are finite, the order q of Q and its index $r = \frac{n}{q}$ in K is finite. Let

$$K = \bigcup_{i=1}^{r} Qb_i$$

be a right coset decomposition of K.

Also only one $b_i = e$ and $b_i \notin Q$ for $i > 1$, so that $Qb_i \neq Q$.

$$HK = A\bigcup_{i=1}^{r} Qb_i$$

$$HK = \bigcup_{i=1}^{r} AQb_i \qquad \ldots(1)$$

Since

$$HQ = \{Hx : x \in Q\} = A$$

So using this in (1), we have

$$HK = \bigcup_{i=1}^{r} Hb_i \qquad \ldots(2)$$

As $b_i \in K$ and $b_i \notin Q$, so b_i's $\notin H$ for $i > 1$.

Therefore, the cosets

$$Hb_i,\ i = 1, 2, \ldots, r$$

are distinct, each of these contains exactly m elements and there are r such cosets, then

$$HK = \bigcup_{i=1}^{r} Ab_i$$

Then by inclusion-exclusion principle, we have

$$\begin{aligned} |HK| &= \sum_{i=1}^{r} |Hb_i| \\ &= |Hb_1| + |Hb_2| + \ldots + |Hb_r| \\ &= r|H| \\ &= rm \\ &= \frac{mn}{q} \qquad \because r = \frac{n}{q} \end{aligned}$$

$$\Rightarrow |HK| = \frac{|H||K|}{|H \cap K|}$$

This completes the proof.

6-6.4 Theorem: *Let H, K be subgroups of a finite group G, then*

$$|HaK| = \frac{|H||K|}{\left|H \cap aKa^{-1}\right|}$$

PU, 2012 (M.Sc. Math)

Alternative Statement:
Let H, K be subgroups of a finite group G, then each double coset HaK contains exactly $\frac{mn}{q}$ *elements, where m, n and q are orders of H, K, and* $Q = H \cap aKa^{-1}$ *respectively.*

Proof: It is given that

$$|H| = m, \quad |K| = n, \quad |H \cap aKa^{-1}| = q$$

Since G is finite, so both H and K are finite and hence, HaK, for $a \in G$ is also finite. Let

$$HaK = \{x_1, x_2, ..., x_r\}$$

where x_i's are distinct.

Now $$HaKa^{-1} = \{x_1a^{-1}, x_2a^{-1}, ..., x_ra^{-1}\}$$

Next we show that x_ia^{-1}'s are distinct. For this suppose on contrary that

$$x_ia^{-1} = x_ja^{-1}, \qquad i \neq j$$

$$(x_ia^{-1})a = (x_ja^{-1})a$$

$$x_i(a^{-1}a) = x_j(a^{-1}a)$$

$$x_ie = x_je \qquad \because a^{-1}a = e$$

$$x_i = x_j$$

Which is a contradiction, so $x_1a^{-1}, x_2a^{-1}, ..., x_ra^{-1}$ are distinct.

Let $K' = aKa^{-1}$, then $|K'| = |aKa^{-1}| = |K|$.

Using the result of previous theorem, we have

$$|HK'| = \frac{|H||K'|}{|H \cap K'|}$$

$$\Rightarrow |HaKa^{-1}| = \frac{|H||K|}{|H \cap aKa^{-1}|} \qquad \because K' = aKa^{-1}, |K'| = |K|$$

$$\Rightarrow |HaK| = \frac{|H||K|}{|H \cap aKa^{-1}|} \qquad \because |HaKa^{-1}| = |HaK|$$

This completes the proof.

6-6.5 Theorem: *Let a group G of order n have subgroups H, K of orders l and m respectively, then*

$$n = \frac{lm}{q_1} + \frac{lm}{q_2} + ... + \frac{lm}{q_r}$$

where q_i *is the order of* $Q_i = H \cap a_iKa_i^{-1}$, $i = 1, 2, 3, ..., r$.

Proof: Since the collection Ω of all double cosets $HaK, a \in G$, is a decomposition of G, i.e.

$$G = \cup Ha_iK,\ a_i \in G$$

$$|G| = \sum_{i=1}^{r} |Ha_iK| \qquad \ldots(1)$$

Since l, m and q_i are the orders of H, K and $Q_i = H \cap a_iKa_i^{-1}$ respectively, so for each i,

$$|Ha_iK| = \frac{lm}{q_i}$$

Using this value in (1), we have

$$|G| = \sum_{i=1}^{r} \frac{lm}{q_i}$$

$$\Rightarrow n = \frac{lm}{q_1} + \frac{lm}{q_2} + \ldots + \frac{lm}{q_r} \qquad \because |G| = n$$

This completes the proof.

6-6.6 Theorem: *Let a HaK be a double coset modulo the subgroups H, K of a group G and $Q = H \cap aKa^{-1}$. Then there is one-to-one correspondence between the left cosets of K that are contained in HaK and the left cosets of the intersection Q of H and aKa^{-1} in H.*

Proof: Let Ω be the collection of all left cosets of K in HaK and Ω' be the collection of all left cosets of Q in H.

Define a mapping $\psi : \Omega \to \Omega'$ by

$$\psi(haK) = hQ$$

(i) Well defined

First we show that ψ is well defined, for this let

$$haK = h_1aK$$

$$\Rightarrow hak = h_1ak_1 \qquad \text{for some } k, k_1 \in K$$

$$\Rightarrow h_1^{-1}hak = ak_1$$

$$\Rightarrow h_1^{-1}ha = ak_1k^{-1}$$

$$\Rightarrow h_1^{-1}h = ak_1k^{-1}a^{-1}$$

$$\Rightarrow h_1^{-1}h \in aKa^{-1} \qquad \because ak_1k^{-1}a^{-1} \in aKa^{-1}$$

$$\Rightarrow h_1^{-1}h \in H \cap aKa^{-1} \qquad \because h_1^{-1}h \in H$$

$$\Rightarrow h_1^{-1}h \in Q \qquad \because H \cap aKa^{-1} = Q$$

$$\Rightarrow h_1^{-1}hQ = Q$$

$$\Rightarrow hQ = h_1Q$$

$$\Rightarrow \psi(haK) = \psi(h_1aK)$$

This shows that ψ is well defined.

(ii) One-One

Next we show that ψ is one-one, for this let

$$\psi(haK) = \psi(h_1aK)$$
$$\Rightarrow hQ = h_1Q$$
$$\Rightarrow h_1^{-1}hQ = Q$$
$$\Rightarrow h_1^{-1}h \in Q$$
$$\Rightarrow h_1^{-1}h \in H \cap aKa^{-1} \quad \because Q = H \cap aKa^{-1}$$
$$\Rightarrow h_1^{-1}h \in aKa^{-1}$$
$$\Rightarrow h_1^{-1}h = aka^{-1} \quad \text{for some } k \in K$$
$$\Rightarrow ha = h_1ak$$
$$\Rightarrow ha \in h_1aK$$

But $ha = hae \in haK$

$$\Rightarrow ha \in haK \cap h_1aK$$
$$\Rightarrow haK = h_1aK \quad \because haK \cap h_1aK \neq \phi$$

This shows that ψ is one-one.

(iii) Onto

Next we show that ψ is onto.

Since for every $hQ \in \Omega'$, there is some $haK \in \Omega$ such that

$$\psi(haK) = hQ$$

This shows that ψ is onto.

This shows that ψ is bijective and it completes the proof.

EXERCISE 6

Multiple Choice Questions (MCQs)

Four options are given in each of the following questions, the choice which you think is correct; fill the circle in front of that choice. Use marker or pen to fill the circles. Cutting or filling two or more circles is not allowed:

Q.1

(i) If X is a complex in V_4, then $N_{V_4}(X) =$

(a) X (b) V_4 (c) ϕ (d) $X \cap V_4$

ⓐ ⓑ ⓒ ⓓ

(ii) If $X = \{a, ab\}$ is a complex in V_4, then $N_{V_4}(X) =$

(a) $\{a, ab\}$ (b) $\{e, a\}$ (c) $\{e, ab\}$ (d) $\{e, a, b, ab\}$

ⓐ ⓑ ⓒ ⓓ

(iii) If X is a complex in a non-abelian group G, then
(a) $N_G(X) = \phi$ (b) $N_G(X) \subseteq G$
(c) $N_G(X) = G$ (d) $G \subseteq N_G(X)$
ⓐ ⓑ ⓒ ⓓ

(iv) If X is a complex in an abelian group G, then
(a) $N_G(X) = \phi$ (b) $N_G(X) \subseteq G$
(c) $N_G(X) = G$ (d) $G \subseteq N_G(X)$
ⓐ ⓑ ⓒ ⓓ

(v) The centre of an abelian group is
(a) an empty set (b) the group itself
(c) $\{e\}$ (d) none of these
ⓐ ⓑ ⓒ ⓓ

(vi) Centre $Z(G)$ of a group G is
(a) abelian subgroup of G (b) non-abelian subgroup of G
(c) an empty set (d) none of these
ⓐ ⓑ ⓒ ⓓ

(vii) If $a, b \in G$, then b is said to be a conjugate of a in G if there exists an element $g \in G$ such that $b =$
(a) ga^4g^{-1} (b) ga^3g^{-1} (c) ga^2g^{-1} (d) gag^{-1}
ⓐ ⓑ ⓒ ⓓ

(viii) If m and n are orders of conjugates elements, then
(a) $m < n$ (b) $m > n$ (c) $m = n$ (d) $m^2 = n$
ⓐ ⓑ ⓒ ⓓ

(ix) V_4 is a p-group, with
(a) $p = 4$ (b) $p = 3$ (c) $p = 1$ (d) $p = 2$
ⓐ ⓑ ⓒ ⓓ

(x) The centre of a finite p-group is
(a) non-nontrivial (b) nontrivial
(c) empty set (d) none of these
ⓐ ⓑ ⓒ ⓓ

Short Questions

Q.2 Solve / answer the following short questions:

(i) Define the complex in a group.
(ii) Define permutable complexes.
(iii) If a nonempty complex H of a group G is a subgroup of G, then show that $HH^{-1} \subseteq H$.
(iv) Define the centre of a group.
(v) Show that centre of an abelian group is the group itself.
(vi) Define the normalizer or centralizer of an element.
(vii) Let G be a group and $a \in G$, then show that $N(a)$ is a subgroup of G.

(viii) Define the normalizer of a complex in a group.
(ix) Define the centralizer of a complex in a group.
(x) Define a double coset in a group.

Long Questions

Q.3 Define the centre $Z(G)$ of a group G. Show that $Z(G)$ is abelian subgroup of G. Also find the centre of S_3.

PU, 2008 (M.Sc. Math)

Q.4 Find the centre of $S_3 = \{e, a, a^2, b, ab, a^2b\}$.

PU, 2008 (M.Sc. Math)

Q.5 Show that the conjugate elements have same order.

Q.6 Show that two conjugate subgroups of a group G have the same order.

Q.7 If H and K are any two conjugate subgroups of a group G, then show that $H \approx K$.

Q.8 Let H, K be subgroups of a finite group G, then show that $o(HK) = \frac{o(H)o(k)}{o(H \cap K)}$.

PU, 2000 (M.Sc. Math)

Q.9 Let H, K be subgroups of a group G and $a \in G$, then show that the collection Ω of all double cosets HaK defines a partition of G.

Q.10 If $S_3 = \{e, a, a^2, b, ab, a^2b\}$ and $X = \{a, b\}$, then find the normalizer of X in S_3.

Q.11 Show that the number of conjugate subgroups of a subgroup H of a group G is equal to the index of the normalizer $N_G(H)$.

SUMMARY

- An arbitrary subset X of a group G is said to be a complex in G.
- Two complexes X and Y in a group G are said to be permutable if $XY = YX$.
- Two complexes X and Y in an abelian group G are permutable.
- A nonempty complex H of a group G is a subgroup of G if and only if $HH^{-1} \subseteq H$.
- A subgroup is a complex but a complex need not be a subgroup.
- If H, K are subgroups of a G, then HK is a subgroup of G if and only if $HK = KH$.
- Centre of a group G is defined as $Z(G) = \{z \in G : zx = xz \; \forall x \in G\}$.
- The centre of an abelian group is the group itself.
- Centre $Z(G)$ of a group G is an abelian subgroup of G.
- $N(a) = \{x \in G : xa = ax\}$ is normalizer or centralizer of a in G.

- $N(a)$ is a subgroup of G.
- Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with X is called normalizer of X in G.
- $N_G(X)$ is always nonempty.
- If G is an abelian group, then $N_G(X) = G$.
- Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with the elements of X is called centralizer of X in G and is denoted by $C_G(X)$.
- $C_G(X)$ is always nonempty.
- If G is an abelian group, then $C_G(X) = G$.
- If $a, b \in G$, then b is said to be a conjugate of a in G if there exists an element $g \in G$ such that $b = g^{-1}ag$.
- Conjugacy between elements of a group is an equivalence relation on G.
- If b is a conjugate of a, then we say that a and b are conjugate elements.
- Set of all those elements of a group G which are conjugate of a in G is called conjugate class of a in G. It is denoted by $C(a)$ or C_a.
- Conjugate elements have same order.
- An element a of a group G is said to be self conjugate if there exists an element $g \in G$ such that $a = g^{-1}ag$.
- If G is a group and $x, y \in G$, $x^{-1}y^{-1}xy$ is called the commutator of x and y or, more briefly, a commutator.
- The number of elements in a conjugacy class C_a of an element a in a group G is equal to the index of its normalizer in G.
- Let G be a finite group and $a \in G$, then the number of elements in a conjugacy class C_a of an element a in G divides the order of G.
- Let H be a subgroup of a group G, then for $g \in G$, gHg^{-1} is called conjugate subgroup of H.
- Two conjugate subgroups of a group G have the same order.
- Any two conjugate subgroups of a group G are isomorphic to each other.
- The number of conjugate subgroups of a subgroup H of a group G is equal to the index of the normalizer $N_G(H)$.
- A group G is said to be a p-group if the order of every element of G can be written as p^{α}, for some fixed p.
- The centre of a finite p-group is nontrivial.
- Let H, K be two subgroups of a group G and $a \in G$, then HaK is called the double coset in G modulo (H,K) determined by a.
- The collection of all double cosets defines a partition of group.

Chapter 7

NORMAL SUBGROUPS

7-1 Normal Subgroups

In this section first of all we shall give the definition of special kind of subgroups and then we will present some important results.

7-1.1 Definition: A subgroup H of a group G is said to be *self conjugate* or *normal subgroup* of G if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

PU, 2014 (BS Math)

We write $H \lhd G$ and read it as: "H is a normal subgroup of G".

Since for each $g \in G$, we have

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

so we can define normal sub group alternatively as follows:

A subgroup H of a group G is said to be *normal subgroup* of G if $gHg^{-1} \subset H$ for all $g \in G$.

Since for any group G, $g \in G \Rightarrow g^{-1} \in G$, so if H is a normal subgroup of G then for any $h \in H$, we have

$$g^{-1}h(g^{-1})^{-1} \in H$$

$$g^{-1}hg \in H \qquad \because (g^{-1})^{-1} = g$$

Consequently, we say that a subgroup H of a group G is said to be *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$.

Equivalently, a subgroup H of a group G is said to be *normal subgroup* of G if $g^{-1}Hg \subset H$ for all $g \in G$.

7-1.2 Theorem:

H is a normal subgroup of G if and only if $gHg^{-1} = H$ *for all* $g \in G$.

Proof: Let H be a normal subgroup of G, then for any $g \in G$, we have

$$gHg^{-1} \subset H \qquad \ldots(1)$$

and

$$g^{-1}Hg \subset H \qquad \ldots(2)$$

From (2), we have

$$g(g^{-1}Hg)g^{-1} \subset gHg^{-1}$$
$$\Rightarrow gg^{-1}Hgg^{-1} \subset gHg^{-1}$$
$$\Rightarrow eHe \subset gHg^{-1} \qquad \because gg^{-1} = e$$
$$\Rightarrow H \subset gHg^{-1} \qquad \ldots(3)$$

Combining (1) and (3), we have

$$gHg^{-1} \subset H \subset gHg^{-1}$$
$$\Rightarrow gHg^{-1} = H$$

Conversely, let $gHg^{-1} = H$ for all $g \in G$, then obviously

$$gHg^{-1} \subset H$$

This shows that H is a normal subgroup of G. This completes the proof.

7-1.3 Theorem: *Every subgroup of an abelian group is its normal subgroup.*

Proof: Let G be an abelian group. Let H be a subgroup of G. Since G is a group, so $g^{-1} \in G$ for any $g \in G$. Since H is a subgroup of G, so $h \in G$ for any $h \in H$. Since G is an abelian group, so

$$ghg^{-1} = gg^{-1}h$$
$$= eh \qquad \because gg^{-1} = e$$
$$= h$$
$$\Rightarrow ghg^{-1} = h \in H$$
$$\Rightarrow ghg^{-1} \in H$$

This shows that H is a normal subgroup of G. This completes the proof.

7-1.4 Theorem: *The subgroup H of G is a normal subgroup of G if and only if every left coset of H in G is a right coset of H in G.*

Proof: Let H be a normal subgroup of G, then for any $g \in G$, we have

$$gHg^{-1} = H$$
$$\Rightarrow (gHg^{-1})g = Hg$$
$$\Rightarrow gHg^{-1}g = Hg$$

$$\Rightarrow gHe = Hg \qquad \because g^{-1}g = e$$
$$\Rightarrow gH = Hg$$

This shows that the left coset gH of H in G is a right coset Hg of H in G.

Conversely, let every left coset of H in G is a right coset of H in G. Thus, for $g \in G$, gH, being a left coset, must be a right coset.

If possible, let

$$gH = Ha \qquad ...(1)$$

for some $a \in G$.

Now

$$g = ge \in gH$$
$$\Rightarrow g \in Ha \qquad \because gH = Ha$$

But

$$g = eg \in Hg$$

This shows that g is in two right costs Ha and Hg, i.e.

$$g \in Ha \cap Hg \qquad ...(2)$$

Since two distinct right cosets have no common points, so (2) is only possible if $Ha = Hg$. Using this in (1), we have

$$gH = Hg$$
$$\Rightarrow gHg^{-1} = (Hg)g^{-1}$$
$$= H(gg^{-1})$$
$$= He \qquad \because gg^{-1} = e$$
$$= H \qquad \because He = H$$

This shows that H is normal subgroup of G.

7-1.5 Definition: Let A, B be subsets of a group G, the *product of sets* A and B is denoted by AB and is defined to be a set

$$AB = \{x \in G : x = ab, a \in A, b \in B\}$$

7-1.6 Theorem:

If H is a subgroup of a group G then $HH = H$.

Proof: Let $h \in H$. Since H is a subgroup of G, so identity element e is in H, i.e. $e \in H$, so

$$h = he \in HH$$
$$\Rightarrow H \subset HH \qquad ...(1)$$

Conversely, let $x \in HH$, then by the definition of product of sets, there are $h_1, h_2 \in H$ such that $x = h_1h_2$.

Since H is a subgroup, so $h_1h_2 \in H$ for $h_1, h_2 \in H$.

Hence

$$x = h_1h_2 \in H$$
$$\Rightarrow HH \subset H \qquad ...(2)$$

Combining (1) and (2), we have

$$HH = H$$

7-1.7 Theorem: *A subgroup H of G is a normal subgroup of G if and only if the product of two right cosets of H in G is again a right coset of H in G.*

Proof: Let H be a normal subgroup of G. Let $a, b \in G$. Next consider the product of two right cosets Ha and Hb of H in G. i.e.

$$(Ha)(Hb) = H(aH)b \qquad ...(1)$$

Since H is a normal subgroup of G, so

$$aH = Ha \qquad ...(2)$$

Using (2) in (1), we have

$$\begin{aligned}(Ha)(Hb) &= H(Ha)b \\ &= HHab \\ &= Hab \qquad \because HH = H\end{aligned}$$

This shows that the product of two right cosets of H in G is again a right coset of H in G.

Conversely, let the product of two right cosets of H in G is again a right coset of H in G, then we have to show that H is a normal subgroup of G. To show that H is normal subgroup of G, let $g \in G$ be any element. Then Hg and Hg^{-1} are two right cosets of H in G. By assumption, Thus $HgHg^{-1}$ is also a right coset of H in G.

If possible, let

$$HgHg^{-1} = Ha \qquad ...(1)$$

for some $a \in G$.

Now

$$\begin{aligned}e = egeg^{-1} &\in HgHg^{-1} \\ \Rightarrow e &\in Ha \qquad \because HgHg^{-1} = Ha\end{aligned}$$

But

$$e \in He$$

This shows that e is in two right costs Ha and He, i.e.

$$e \in Ha \cap He \qquad ...(2)$$

Since two distinct right cosets have no common points, so (2) is only possible if $Ha = He$. Using this in (1), we have

$$\begin{aligned}HgHg^{-1} &= He \\ \Rightarrow HgHg^{-1} &= H \qquad \because He = H\end{aligned}$$

It is obvious that for all $h_1, h \in H, g \in G$,

$$\begin{aligned}h_1ghg^{-1} &\in HgHg^{-1} \\ \Rightarrow h_1ghg^{-1} &\in H \qquad \because HgHg^{-1} = H \\ \Rightarrow h_1^{-1}(h_1ghg^{-1}) &\in H \qquad \because H \text{ is subgroup}\end{aligned}$$

$$\Rightarrow (h_1^{-1}h_1)ghg^{-1} \in H$$

$$\Rightarrow (e)ghg^{-1} \in H \qquad \because h_1^{-1}h_1 = e$$

$$\Rightarrow ghg^{-1} \in H \qquad \because (e)ghg^{-1} = ghg^{-1}$$

This shows that H is a normal subgroup of G.

7-1.8 Theorem: *If G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G.*

PU, 2008 (M.Sc. Math)

Proof: Let H be a subgroup of G, with index 2, then number of different right (left) cosets of H in G is 2 and also then G is union of these two right (left) cosets.

Let $g \in G$ be arbitrary.

Case-I: If $g \in H$, then $Hg = H = gH$, i.e.

$$Hg = gH$$

Hence H is normal subgroup of G.

Case-II: If $g \notin H$ then $gH \neq H$, $Hg \neq H$.

Thus Hg and $H = He$ are the two distinct right cosets of H in G and

$$G = Hg \cup H \qquad ...(1)$$

Similarly,

$$G = gH \cup H \qquad ...(2)$$

Equating (1) and (2), we have

$$Hg \cup H = gH \cup H$$

$$\Rightarrow Hg = gH \qquad \because Hg \cap H = \phi = gH \cap H$$

Hence H is normal subgroup of G.

7-1.9 Theorem: *The intersection of two normal subgroups of G is a normal subgroup of G.*

PU, 2015 (BS Math)

Proof: Let H, K be two normal subgroups of G. Let

$$N = H \cap K$$

We have to show that N is a normal subgroup of G. For this let $g \in G$, $n \in N$. Now

$$n \in N$$

$$\Rightarrow n \in H \cap K \qquad \because N = H \cap K$$

$$\Rightarrow n \in H \text{ and } n \in K$$

$$\Rightarrow gng^{-1} \in H \text{ and } gng^{-1} \in K \qquad \because H, K \text{ are normal}$$

$$\Rightarrow gng^{-1} \in H \cap K$$

$$\Rightarrow gng^{-1} \in N$$

This shows that N is normal subgroup of G.

Hence, the intersection of two normal subgroups of G is a normal subgroup of G.

7-1.10 Theorem: *The intersection of any number of normal subgroups of G is a normal subgroup of G.*

Proof: Let $\{H_\alpha : \alpha \in \Omega\}$ be a collection of normal subgroups of G. Let

$$H = \bigcap_{\alpha\in\Omega} H_\alpha$$

We have to show that H is a normal subgroup of G. For this let $g \in G$, $h \in H$. Now

$$h \in H$$
$$\Rightarrow h \in \bigcap_{\alpha\in\Omega} H_\alpha \qquad \because H = \bigcap_{\alpha\in\Omega} H_\alpha$$
$$\Rightarrow h \in H_\alpha \quad \text{for every } \alpha \in \Omega$$
$$\Rightarrow ghg^{-1} \in H_\alpha \quad \text{for every } \alpha \in \Omega \qquad \because \text{all } H_\alpha \text{ are normal}$$
$$\Rightarrow ghg^{-1} \in \bigcap_{\alpha\in\Omega} H_\alpha$$
$$\Rightarrow ghg^{-1} \in H$$

This shows that H is normal subgroup of G.
Hence, the intersection of any number of normal subgroups of G is a normal subgroup of G.

7-1.11 Theorem: *If H is a subgroup of a group G such that $(aH)(Hb)$ for any $a, b \in G$ is either a left or a right coset of H in G then H is normal.*

Proof: Let $a \in G$ be any element.

Now
$$e = aeea^{-1}$$
$$= (ae)(ea^{-1}) \in aHHa^{-1}$$

Also $e \in H = He = eH$

Thus $(aH)(Ha^{-1})$ and H are two right (left) cosets of H in G and contain a common clement e. This shows that

$$(aH)(Ha^{-1}) = H$$
$$\Rightarrow aHHa^{-1} = H$$
$$\Rightarrow aHa^{-1} = H \quad \because HH = H$$

Hence, H is a normal subgroup of G.

7-1.12 Theorem: *If H and K are two normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H, k \in K$.*

PU, 2009; 2003 (M.Sc. Math)

Proof: Let $h \in H, k \in K$ be any elements, then

$$h \in H, k \in K \subset G$$

Since H is normal in G, so

$$k^{-1}hk \in H$$
$$\Rightarrow k^{-1}hkh^{-1} \in H$$

Similarly, $h^{-1} \in H \subset G, k \in K$

Since K is normal in G, so

$$(h^{-1})^{-1} k h^{-1} \in K$$
$$\Rightarrow hkh^{-1} \in K$$
$$\Rightarrow k^{-1}hkh^{-1} \in K$$
$$\Rightarrow k^{-1}hkh^{-1} \in H \cap K$$
$$\Rightarrow k^{-1}hkh^{-1} = e \qquad \because H \cap K = \{e\}$$
$$\Rightarrow k(k^{-1}hkh^{-1})h = keh$$
$$\Rightarrow kk^{-1}(hk)h^{-1}h = kh$$
$$\Rightarrow e(hk)e = kh \qquad \because kk^{-1} = e = h^{-1}h$$
$$\Rightarrow hk = kh$$

7-1.13 Theorem: *If a cyclic subgroup K of G is normal in G then every subgroup of K is normal in G.*

Proof: Since K is cyclic, so let it be generated by a. Let H be any subgroup of K. We have to show that H is a normal subgroup of G.

Since H is the subgroup of a cyclic group K, so H itself is cyclic. Let a^m be the generator of H. Let $g \in G$ and $h \in H$ be any elements then

$$h = (a^m)^n$$

for some integer n, therefore,

$$g^{-1}hg = g^{-1}(a^m)^n g$$
$$= g^{-1}(a^n)^m g$$
$$= (g^{-1}a^n g)^m \qquad \because g^{-1}(a^n)^m g = (g^{-1}a^n g)^m$$

Since $K = < a >$, so $a^n \in K$ and as K is normal in G, so

$$g^{-1}a^n g \in K$$
$$\Rightarrow g^{-1}a^n g = a^t \quad \text{for some integer } t$$
$$\Rightarrow (g^{-1}a^n g)^m = (a^t)^m$$
$$\Rightarrow g^{-1}hg = (a^m)^t \qquad \because (g^{-1}a^n g)^m = g^{-1}hg$$
$$\Rightarrow g^{-1}hg = (a^m)^t \in H \quad \because H = < a^m >$$
$$\Rightarrow g^{-1}hg \in H$$

This shows that H is normal in G.
Hence, every subgroup of K is normal in G.

7-1.14 Example:
Show that a subgroup H of G is normal iff $xy \in H \Rightarrow yx \in H$.

Solution:
Let H be a normal subgroup G and let $xy \in H$. Since H is normal in G and $xy \in H, y \in G$, so

$$y(xy)y^{-1} \in H$$
$$\Rightarrow (yx)yy^{-1} \in H$$
$$\Rightarrow (yx)e \in H \qquad \because yy^{-1} = e$$
$$\Rightarrow yx \in H$$

Conversely, let $xy \in H \Rightarrow yx \in H$, then we have to show that H is normal in G. For this, let $h \in H, g \in G$ be any elements, then

$$h \in H$$
$$\Rightarrow he \in H$$
$$\Rightarrow h(gg^{-1}) \in H \qquad \because gg^{-1} = e$$
$$\Rightarrow (hg)g^{-1} \in H$$
$$\Rightarrow g^{-1}(hg) \in H \qquad \text{(by given condition)}$$
$$\Rightarrow g^{-1}hg \in H$$

This shows that H is a normal subgroup of G.

7-1.15 Example:

Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$, then show that N is a normal subgroup of G.

Solution: Since H is a subgroup of G, so for any $x \in G$, the subsets of the type xHx^{-1} are also subgroups of G. Since the intersection of subgroups is a subgroup, so $\bigcap_{x \in G} xHx^{-1}$ is a subgroup of G.

Let $g \in G$ be any element, then

$$gN = g(\bigcap_{x \in G} xHx^{-1})$$
$$= \bigcap_{x \in G} gxHx^{-1} \qquad \because g(H \cap K) = gH \cap gK$$
$$\Rightarrow gNg^{-1} = (\bigcap_{x \in G} gxHx^{-1})g^{-1}$$
$$= \bigcap_{x \in G} gxHx^{-1}g^{-1} \qquad \because (H \cap K)g^{-1} = Hg^{-1} \cap Kg^{-1}$$
$$= \bigcap_{y \in G} yHy^{-1} \qquad (y = gx \in G)$$
$$= N \qquad \because \bigcap_{y \in G} yHy^{-1} = N$$

This shows that N is a normal subgroup of G.

7-1.16 Theorem: *Let a be an element of order 2 in a group G, then $H = < a : a^2 = e >$ is normal in G if and only if $a \in Z(G)$.*

Proof: For any $g \in G$

$$H \text{ is normal in } G \Leftrightarrow gH = Hg$$
$$\Leftrightarrow g\{e,a\} = \{e,a\}g$$
$$\Leftrightarrow \{ge,ga\} = \{eg,ag\}$$
$$\Leftrightarrow \{g,ga\} = \{g,ag\}$$
$$\Leftrightarrow ga = ag$$
$$\Leftrightarrow a \in Z(G)$$

This completes the proof.

7-1.17 Theorem: *If H and K are normal subgroups of a group G, then HK is a normal subgroup of G.*

PU, 2015 (BS Math); PU, 2008; 2005; 2000 (M.Sc. Math)

Proof: Let $x \in HK$, then $x = hk, h \in H, k \in K$.

For any $g \in G$, consider

$$gxg^{-1} = g(hk)g^{-1} \qquad \because x = hk$$
$$= ghekg^{-1}$$
$$= ghg^{-1}gkg^{-1} \quad \because g^{-1}g = e$$
$$= (ghg^{-1})(gkg^{-1})$$

Since H and K are normal in G, so for $g \in G$,

$$ghg^{-1} \in H,\ gkg^{-1} \in K$$
$$\Rightarrow (ghg^{-1})(gkg^{-1}) \in HK$$
$$\Rightarrow gxg^{-1} \in HK \qquad \because (ghg^{-1})(gkg^{-1}) = gxg^{-1}$$

This shows that HK is normal in G.

7-1.18 Theorem: *If H is a subgroup of a group G, then H is a normal subgroup of $N_G(H)$.*

Proof: We know that $N_G(H)$ is always a subgroup of G.

Also $N_G(H) = \{g \in G : gH = Hg\}$

Since for all $h \in H$, we have

$$hH = H = Hh$$
$$\Rightarrow h \in N_G(H)$$
$$\Rightarrow H \subseteq N_G(H)$$

This shows that H is a subset of $N_G(H)$.

Since for any $x \in N_G(H)$

$$\Rightarrow xH = Hx$$

Hence, H is a normal subgroup of $N_G(H)$.

7-1.19 Theorem: *The centralizer of a normal subgroup H of a group G is normal in G.*

Proof: The centralizer of a subgroup H is given by

$$C_G(H) = \{g \in G : gh = hg, h \in H\}$$

Since H is normal in G, so for each $h \in H, g \in G$, there exists some $h' \in H$ such that

$$hg = gh'$$
$$\Rightarrow g^{-1}h = h'g^{-1}$$

Let $x \in C_G(H)$ and consider

$$\begin{aligned} h(gxg^{-1}) &= (hg)(xg^{-1}) \\ &= (gh')(xg^{-1}) && \because hg = gh' \\ &= g(h'x)g^{-1} \\ &= g(xh')g^{-1} && \because x \in C_G(H) \therefore xh' \text{ for } h' \in H \\ &= (gx)(h'g^{-1}) \\ &= (gx)(g^{-1}h) && \because h'g^{-1} = g^{-1}h \\ &= (gxg^{-1})h \end{aligned}$$

$$\Rightarrow gxg^{-1} \in C_G(H)$$
$$\Rightarrow C_G(H) \lhd G$$

This shows that $C_G(H)$ is normal in G.

7-1.20 Theorem: *The following statements about a subgroup H of a group G are equivalent:*

(a) *H is normal subgroup of G.*

(b) *The normalizer of H in G is G, i.e. $N_G(H) = G$.*

(c) *Any left coset of H in G is equal to its corresponding right coset in G, i.e. $gH = Hg$ for all $g \in G$.*

(d) *For each $h \in H$ and any $g \in G$, $ghg^{-1} \in H$.*

Proof:

$(a) \Rightarrow (b)$: Let H be a normal subgroup of G, then for all $g \in G$, we have

$$gH = Hg$$
$$\Rightarrow g \in N_G(H)$$
$$\Rightarrow G \subseteq N_G(H)$$

But $N_G(H) \subseteq G$

Therefore, $N_G(H) = G$

$(b) \Rightarrow (c)$: Let $N_G(H) = G$, let $g \in G$, then $g \in N_G(H)$, so

$$gH = Hg$$

This shows that any left coset of H in G is equal to its corresponding right coset in G.

$(c) \Rightarrow (d)$: Let $gH = Hg$ for all $g \in G$. Now

$$gH = Hg$$
$$\Rightarrow gh = h'g \quad \text{for some } h, h' \in H$$
$$\Rightarrow ghg^{-1} = h'$$
$$\Rightarrow ghg^{-1} \in H \quad \because h' \in H$$

$(d) \Rightarrow (a)$: Let $ghg^{-1} \in H$, for each $h \in H$ and any $g \in G$, then it fulfils the definition of a normal set, so H is normal in G.
This completes the proof.

7-2 Quotient or Factor Groups

Let G be a group and N a normal subgroup of G. Let $\frac{G}{N}$ be a collection of all the right cosets of N in G.

Next we show that $\frac{G}{N}$ is a group with respect to product of sets.

G_1): Let $X, Y \in \frac{G}{N}$, then for some $a, b \in G$, $X = Na$, $Y = Nb$, because $\frac{G}{N}$ consists of all right cosets of N in G.

Since N is normal subgroup of G, so $NaNb = Nab$. Since Nab is a right coset of N in G, so $Nab \in \frac{G}{N}$.

This shows that

$$XY = NaNb = Nab \in \frac{G}{N}$$

This shows that closure law holds in $\frac{G}{N}$.

G_2): Let $X, Y, Z \in \frac{G}{N}$, then for some $a, b, c \in G$

$X = Na$, $Y = Nb$, $Z = Nc$

Next consider

$$X(YZ) = Na(NbNc)$$
$$= Na(Nbc) \quad \because NbNc = Nbc$$
$$= Nabc \quad \because Na(Nbc) = Nabc$$
$$= (Nab)Nc$$
$$= (NaNb)Nc = (XY)Z$$

This shows that associative law holds in $\frac{G}{N}$.

G_3): Since Ne is a right coset of N in G, so $Ne \in \frac{G}{N}$ such that

$$NaNe = Nae = Na$$
$$NeNa = Nea = Na$$

for every $Na \in \frac{G}{N}$.

This shows that Ne is an identity element of $\frac{G}{N}$, so identity law holds in $\frac{G}{N}$.

G_4): Let $X \in \frac{G}{N}$, then for some $a \in G$, $X = Na$, because $\frac{G}{N}$ consists of all right cosets of N in G.

Since G is a group and $a \in G$, so $a^{-1} \in G$. Then Na^{-1}, being the right coset of N in G, is in $\frac{G}{N}$, i.e. $Na^{-1} \in \frac{G}{N}$ such that

$$\begin{aligned}(Na)(Na^{-1}) &= NaNa^{-1}\\ &= Naa^{-1}\\ &= Ne\end{aligned}$$

$$\begin{aligned}(Na^{-1})(Na) &= Na^{-1}Na\\ &= Na^{-1}a\\ &= Ne\end{aligned}$$

This shows that Na^{-1} is an inverse of Na^{-1}, so inverse of each element of $\frac{G}{N}$ is in $\frac{G}{N}$.

Since all the axioms of a group are satisfied, so $\frac{G}{N}$ is a group. It is called the *quotient group* or *factor group* of G by N.
Thus, we can write

$$\frac{G}{N} = \{Ng : g \in G\}$$

Similarly, we can also show that the set of all left cosets of N in G is also a group with respect to product of sets.

Thus,

$$\frac{G}{N} = \{gN : g \in G\}$$

is also a *quotient group* or *factor group*.

7-2.1 Example: *If* $V_4 = \{e, a, b, ab\}$ *and* $N = \{e, a\}$ *the normal subgroup of* V_4. *Find the quotient group* $\frac{V_4}{N}$.

Solution: We find all left cosets of N in G as follows:

$$eN = e\{e, a\} = \{ee, ea\} = \{e, a\} = N$$
$$aN = a\{e, a\} = \{ae, aa\} = \{e, a\} = N$$
$$bN = b\{e, a\} = \{be, ba\} = \{b, ab\} = N_1$$
$$abN = ab\{e, a\} = \{abe, aba\} = \{ab, b\} = N_1$$

Thus, $\frac{V_4}{N} = \{N, N_1\}$.

7-2.2 Example: *If* G *is an abelian group and* N *is a normal subgroup of* G *then show that* $\frac{G}{N}$ *is an abelian group with respect to product of sets.*

PU, 2014 (BS Math)

Proof: We have already shown that $\frac{G}{N}$ is a group with respect to product of sets. We now show that commutative law holds in $\frac{G}{N}$.

For this let, $X, Y \in \frac{G}{N}$, then for some $a, b \in G$, $X = Na$, $Y = Nb$, because $\frac{G}{N}$ consists of all right cosets of N in G. Next consider

$$\begin{aligned} XY &= NaNb \\ &= Nab \\ &= Nba \qquad \because G \text{ is abelian } \therefore ab = ba \\ &= NbNa \\ &= YX \end{aligned}$$

This shows that $\frac{G}{N}$ is an abelian group.

7-2.3 Theorem: *If* G *is an abelian group and* N *is a normal subgroup of* G *Suppose* G *is a group,* N *a normal subgroup of* G; *define the mapping* ϕ *from* G *to* $\frac{G}{N}$ *by* $\phi(x) = Nx$ *for all* $x \in G$. *Then* ϕ *is a homomorphism of* G *onto* $\frac{G}{N}$.

Proof: First we show that ϕ is onto. For this let $X \in \frac{G}{N}$ be any element of

$\frac{G}{N}$, then by the definition of $\frac{G}{N}$, there must exist an element $x \in G$ such that

$$X = Nx$$
$$= \phi(x) \qquad \because \phi(x) = Nx$$

This shows that X is an image of an element x of G under ϕ. Similarly, we can show that each element of $\frac{G}{N}$ is an image of some element of G under ϕ. This shows that

$$\phi : G \to \frac{G}{N}$$

defined by

$$\phi(x) = Nx \text{ for all } x \in G$$

is onto mapping. Next suppose $x, y \in G$ and consider

$$\phi(xy) = Nxy$$
$$= NxNy \qquad \because Nxy = NxNy$$
$$= \phi(x)\phi(y)$$

This shows that ϕ is a homomorphism of G onto $\frac{G}{N}$.

7-2.4 Definition: Let G and G' be two groups. Let $\phi : G \to G'$ be a homomorphism, the *kernel of homomorphism* is denoted by K_ϕ and is defined as

$$K_\phi = \{x \in G : \phi(x) = e'\}$$

where e' is an identity element of G'.

7-2.5 Theorem: *Let G and G' be two groups and $\phi : G \to G'$ is a homomorphism then kernel of homomorphism is a normal subgroup of G.*

PU, 2003 (M.Sc. Math)

Proof: First we show that the kernel of homomorphism, K_ϕ, is a subgroup of G. For this let $x, y \in K_\phi$, then by the definition K_ϕ, we have

$$\phi(x) = e', \ \phi(y) = e'$$

where e' is an identity element of group G'.
Next consider

$$\phi(xy^{-1}) = \phi(x) \cdot \phi(y^{-1}) \qquad \because \phi \text{ is a homomorphi sm}$$
$$= \phi(x) \cdot (\phi(y))^{-1} \qquad \because \phi(y^{-1}) = (\phi(y))^{-1}$$
$$= e' \cdot (e')^{-1} \qquad \because \phi(x) = e', \phi(y) = e'$$
$$= e' \cdot e' = e' \qquad \because (e')^{-1} = e', e' \cdot e' = e'$$

$$\Rightarrow xy^{-1} \in K_\phi$$

This shows that K_ϕ is a subgroup of G.

Next we show that K_ϕ is normal in G. For this let $x \in K_\phi$, then $\phi(x) = e'$. For any $g \in G$, consider

$$\begin{aligned}\phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1}) && \because \phi \text{ is a homomorphi sm}\\ &= \phi(g)e'(\phi(g))^{-1} && \because \phi(g^{-1}) = (\phi(g))^{-1}\\ &= \phi(g)(\phi(g))^{-1}\\ &= e'\end{aligned}$$

$$\Rightarrow gxg^{-1} \in K_\phi$$

This shows that K_ϕ is a normal subgroup of G.

7-3 Fundamental Theorems of Homomorphism

7-3.1 First Fundamental Theorem of Homomorphism:

Let G and G' be two groups. Let $\phi : G \to G'$ be an epimorphism, then $\frac{G}{K_\phi} \approx G'$.

Proof: First we show that K_ϕ, is a subgroup of G. For this let $x, y \in K_\phi$, then by the definition K_ϕ, we have PU, 2010 (M.Sc. Math)

$$\phi(x) = e', \ \phi(y) = e'$$

where e' is an identity element of group G'.
Next consider

$$\begin{aligned}\phi(xy^{-1}) &= \phi(x)\cdot\phi(y^{-1}) && \because \phi \text{ is a homomorphi sm}\\ &= \phi(x)\cdot(\phi(y))^{-1} && \because \phi(y^{-1}) = (\phi(y))^{-1}\\ &= e'\cdot(e')^{-1} && \because \phi(x) = e', \phi(y) = e'\\ &= e'\cdot e' = e' && \because (e')^{-1} = e', e'\cdot e' = e'\end{aligned}$$

$$\Rightarrow xy^{-1} \in K_\phi$$

This shows that K_ϕ is a subgroup of G.

Next we show that K_ϕ is normal in G. For this let $x \in K_\phi$, then $\phi(x) = e'$. For any $g \in G$, consider

$$\begin{aligned}\phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1}) && \because \phi \text{ is a homomorphi sm}\\ &= \phi(g)e'(\phi(g))^{-1} && \because \phi(g^{-1}) = (\phi(g))^{-1}\end{aligned}$$

$$\phi(gxg^{-1}) = \phi(g)(\phi(g))^{-1}$$
$$= e'$$
$$\Rightarrow gxg^{-1} \in K_\phi$$

This shows that K_ϕ is a normal subgroup of G.

Next we show that $\frac{G}{K_\phi} \approx G'$. For this we define a mapping

$$\psi : \frac{G}{K_\phi} \to G'$$

by

$$\psi(gK_\phi) = g' = \phi(g)$$

(i) Well defined

First we show that ψ is well defined, for this let

$$g_1K_\phi = g_2K_\phi$$
$$\Rightarrow g_2^{-1}g_1K_\phi = K_\phi$$
$$\Rightarrow g_2^{-1}g_1 \in K_\phi$$
$$\Rightarrow \phi(g_2^{-1}g_1) = e'$$
$$\Rightarrow \phi(g_2^{-1})\phi(g_1) = e' \qquad \because \phi \text{ is a homomorphi sm}$$
$$\Rightarrow (\phi(g_2))^{-1}\phi(g_1) = e' \qquad \because \phi(g_2^{-1}) = (\phi(g_2))^{-1}$$
$$\Rightarrow \phi(g_1) = e'\phi(g_2)$$
$$\Rightarrow \phi(g_1) = \phi(g_2)$$
$$\Rightarrow \psi(g_1K_\phi) = \psi(g_2K_\phi)$$

This shows that ψ is well defined.

(ii) One-One

Next we show that ψ is one-one, for this let

$$\psi(g_1K_\phi) = \psi(g_2K_\phi)$$
$$\Rightarrow \phi(g_1) = \phi(g_2)$$
$$\Rightarrow (\phi(g_2))^{-1}\phi(g_1) = e'$$
$$\Rightarrow \phi(g_2^{-1})\phi(g_1) = e' \qquad \because \phi(g_2^{-1}) = (\phi(g_2))^{-1}$$
$$\Rightarrow \phi(g_2^{-1}g_1) = e' \qquad \because \phi \text{ is a homomorphi sm}$$
$$\Rightarrow g_2^{-1}g_1 \in K_\phi$$
$$\Rightarrow g_2^{-1}g_1K_\phi = K_\phi$$
$$\Rightarrow g_1K_\phi = g_2K_\phi$$

This shows that ψ is one-one.

(iii) Onto

Next we show that ψ is onto.

For every $g' \in G'$, there is some $gK_\phi \in \frac{G}{K_\phi}$ such that $\psi(gK_\phi) = g'$.

This shows that ψ is onto.

(iv) Homomorphism

Next we show that ψ is a homomorphism, for this consider

$$\begin{aligned}\psi(g_1K_\phi \cdot g_2K_\phi) &= \psi(g_1g_2K_\phi) \quad \because g_1K_\phi \cdot g_2K_\phi = g_1g_2K_\phi \\ &= \phi(g_1g_2) \\ &= \phi(g_1)\phi(g_2) \quad \because \phi \text{ is a homomorphism} \\ &= \psi(g_1K_\phi)\psi(g_2K_\phi)\end{aligned}$$

This shows that ψ is a homomorphism.

Now ψ, being bijective homomorphism, is an isomorphism, so $\frac{G}{K_\phi} \approx G'$.

This completes the proof.

7-3.2 Second Fundamental Theorem of Homomorphism:

Let H be a normal subgroup of a group G and K a subgroup of G, then $\frac{HK}{H} \approx \frac{K}{H \cap K}$.

PU, 2015 (BS Math); PU, 2012; 2010; 2008; 2007; 2006; 2005 (M.Sc. Math)

Proof:

First of all we have to show that the quotient groups $\frac{HK}{H}$ and $\frac{K}{H \cap K}$ are well defined. To show that the factor groups $\frac{HK}{H}$ and $\frac{K}{H \cap K}$ are well defined, we have to show that HK is a subgroup of G and $H \cap K$ is a normal subgroup of K.

First we show that HK is a subgroup of G, for this let

$$\begin{aligned}&x, y \in HK \\ \Rightarrow\ & x = h_1k_1,\ y = h_2k_2, \quad h_1, h_2 \in H, k_1, k_2 \in K \\ \text{Now } xy^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= (h_1k_1)(k_2^{-1}h_2^{-1}) \\ &= h_1(k_1k_2^{-1})h_2^{-1} \\ &= h_1(k_3h_2^{-1}) \qquad (k_3 = k_1k_2^{-1} \in K) \\ &= h_1(h_2^{-1}k_3) \quad \because H \text{ is normal } \therefore k_3h_2^{-1} = h_2^{-1}k_3 \\ &= (h_1h_2^{-1})k_3\end{aligned}$$

$$\Rightarrow xy^{-1} \in HK \qquad \because (h_1h_2^{-1})k_3 \in HK$$

This shows that HK is a subgroup of G.

Next we show that $H \cap K$ is normal in K. For this let

$$x \in H \cap K, \quad k \in K$$
$$\Rightarrow x \in H \text{ and } x \in K$$
$$\Rightarrow kxk^{-1} \in H \text{ and } kxk^{-1} \in K \qquad \because H \lhd G$$
$$\Rightarrow kxk^{-1} \in H \cap G$$

This shows that $H \cap K$ is normal is normal in K.

As H is already subgroup of G, so to show that H is a subgroup of HK, it is enough to show that H is a subset of HK. For this let

$$h \in H$$
$$\Rightarrow he \in HK \qquad \because e \in K$$
$$\Rightarrow h \in HK \qquad \because he = h$$
$$\Rightarrow H \subseteq HK$$

This shows that H is a subgroup of HK. Since H is normal in G, so it is normal in HK.

Since H is a normal subgroup of HK, so the quotient group $\frac{HK}{H}$ is well defined.

Similarly, since $H \cap K$ is normal in K, so the quotient group $\frac{K}{H \cap K}$ is well defined.

We observe that

$$\frac{HK}{H} = \{(hk)^{-1}H : h \in H, k \in K\}$$
$$= \{k^{-1}h^{-1}H : h \in H, k \in K\}$$
$$= \{k^{-1}H : k \in K\} \qquad \because h^{-1}H = H$$

This shows that the elements of $\frac{HK}{H}$ are of the form kH.

Finally, let $D = H \cap K$ and define a mapping

$$\phi : \frac{HK}{H} \to \frac{K}{D}$$

by $$\phi(kH) = kD$$

(i) Well defined

First we show that ϕ is well defined, for this let

$$k_1H = k_2H$$
$$\Rightarrow k_2^{-1}k_1H = H$$
$$\Rightarrow k_2^{-1}k_1 \in H$$

$$\Rightarrow k_2^{-1}k_1 \in H \cap K \qquad \because k_2^{-1}k_1 \in K$$
$$\Rightarrow k_2^{-1}k_1 \in D \qquad \because H \cap K = D$$
$$\Rightarrow k_2^{-1}k_1 D \in D$$
$$\Rightarrow k_1 D \in k_2 D$$
$$\Rightarrow \phi(k_1 H) = \phi(k_2 H)$$

This shows that ϕ is well defined.

(ii) One-One

Next we show that ϕ is one-one, for this let

$$\phi(k_1 H) = \phi(k_2 H)$$
$$\Rightarrow k_1 D \in k_2 D$$
$$\Rightarrow k_2^{-1}k_1 D \in D$$
$$\Rightarrow k_2^{-1}k_1 \in D$$
$$\Rightarrow k_2^{-1}k_1 \in H \cap K \qquad \because H \cap K = D$$
$$\Rightarrow k_2^{-1}k_1 \in H \text{ and } k_2^{-1}k_1 \in K$$
$$\Rightarrow k_2^{-1}k_1 H = H \qquad \because k_2^{-1}k_1 \in H$$
$$\Rightarrow k_1 H = k_2 H$$

This shows that ϕ is one-one.

(iii) Onto

Next we show that ϕ is onto.

For every $kD \in \frac{K}{D}$, there is some $kH \in \frac{HK}{H}$ such that $\phi(kH) = kD$.

This shows that ϕ is onto.

(iv) Homomorphism

Next we show that ϕ is a homomorphism, for this consider

$$\phi(k_1 H \cdot k_2 H) = \phi(k_1 k_2 H) \qquad \because H \text{ is normal } \therefore k_1 H \cdot k_2 H = k_1 k_2 H$$
$$= k_1 k_2 D$$
$$= k_1 D \cdot k_2 D \qquad \because D \text{ is normal } \therefore k_1 k_2 D = k_1 D \cdot k_2 D$$
$$= \phi(k_1 H)\phi(k_2 H)$$

This shows that ϕ is a homomorphism.

Now ϕ, being bijective homomorphism, is an isomorphism, so $\frac{HK}{H} \approx \frac{K}{D}$,

i.e. $\frac{HK}{H} \approx \frac{K}{H \cap K}$.

This completes the proof.

7-3.3 Third Fundamental Theorem of Homomorphism:

Let H, K be normal subgroups of a group G and $H \subseteq K$, then $\frac{G}{K} \approx \frac{G/H}{K/H}$.

PU, 2011 (M.Sc. Math)

Proof: The subgroup H, being a normal subgroup of G, is normal in any subgroup of G containing H, so H is normal in K.

To prove this theorem, we will use first fundamental theorem of homomorphism. For this first we show that

$$\phi : \frac{G}{H} \to \frac{G}{K}$$

is an epimorphism and $\frac{K}{H} = K_\phi$.

Define $\phi : \frac{G}{H} \to \frac{G}{K}$

by $\phi(gH) = gK$

(i) Well defined

First we show that ϕ is well defined, for this let

$$\begin{aligned} & g_1H = g_2H \\ \Rightarrow\ & g_2^{-1}g_1H = H \\ \Rightarrow\ & g_2^{-1}g_1 \in H \\ \Rightarrow\ & g_2^{-1}g_1 \in K \quad \because H \subseteq K \\ \Rightarrow\ & g_2^{-1}g_1K = K \\ \Rightarrow\ & g_1K = g_2K \\ \Rightarrow\ & \phi(g_1H) = \phi(g_2H) \end{aligned}$$

This shows that ϕ is well defined.

(ii) Onto

Next we show that ϕ is onto.

For every $gK \in \frac{G}{K}$, there is some $gH \in \frac{G}{H}$ such that $\phi(gH) = gK$.

This shows that ϕ is onto.

(iii) Homomorphism

Next we show that ϕ is a homomorphism, for this consider

$$\begin{aligned} \phi(g_1H \cdot g_2H) &= \phi(g_1g_2H) && \because H \text{ is normal } \therefore g_1H \cdot g_2H = g_1g_2H \\ &= g_1g_2K \\ &= g_1K \cdot g_2K && \because K \text{ is normal } \therefore g_1g_2K = g_1K \cdot g_2K \\ &= \phi(g_1H)\phi(g_2H) \end{aligned}$$

This shows that ϕ is a homomorphism.

Let $x \in \frac{K}{H}$

$\Rightarrow x = kH$ for some $k \in K$

$\Rightarrow \phi(x) = \phi(kH)$

$= kK$ $\because \phi(kH) = kK$

$= K$ $\because kK = K$

Since ϕ is a homomorphism form a group $\frac{G}{H}$ to a group $\frac{G}{K}$ and $\frac{G}{K}$ consists of all left cosets of K in G, therefore, K itself will play the role of an identity element of $\frac{G}{K}$, so

$$\phi(x) = K$$
$$\Rightarrow x \in K_\phi$$
$$\Rightarrow \frac{K}{H} \subseteq K_\phi \quad \ldots(1)$$

Conversely, let

$$xH \in K_\phi$$
$$\Rightarrow \phi(xH) = K$$
$$\Rightarrow xK = K \quad \because \phi(xH) = xK$$
$$\Rightarrow x \in K$$
$$\Rightarrow xH \in \frac{K}{H}$$
$$\Rightarrow K_\phi \subseteq \frac{K}{H} \quad \ldots(2)$$

Combining (1) and (2), we have

$$K_\phi = \frac{K}{H}$$

We have proved that $\phi : \frac{G}{H} \to \frac{G}{K}$ is an epimorphism, so by First Theorem of Homomorphism, we have

$$\frac{G/H}{K_\phi} \approx \frac{G}{K} \quad \ldots(3)$$

Since $K_\phi = \frac{K}{H}$, so (3) takes the from

$$\frac{G/H}{K/H} \approx \frac{G}{K}$$

or

$$\frac{G}{K} \approx \frac{G/H}{K/H}$$

7-3.4 Theorem: *A group G is abelian if and only if the factor group is $\frac{G}{Z(G)}$ is cyclic.*

PU, 2007; 2005; 2002 (M.Sc. Math)

Proof: Let G be abelian, then $Z(G) = G$, so

$$\frac{G}{Z(G)} = \frac{G}{G} = G$$

In order to show that $\frac{G}{Z(G)}$ is cyclic, we have to show that each element of $\frac{G}{Z(G)}$ is generated by its some fixed element.

For this let $aZ(G) \in \frac{G}{Z(G)}$, and consider

$$(aZ(G))^m = a^m Z(G) \in \frac{G}{Z(G)}$$

This shows that each element of $\frac{G}{Z(G)}$ can be taken as a power of a, so $\frac{G}{Z(G)}$ is cyclic.

Since $\frac{G}{Z(G)}$ consists of left cosets of $Z(G)$ in G, so $aZ(G) \in \frac{G}{Z(G)}$

Conversely, let $\frac{G}{Z(G)}$ be a cyclic group generated by $aZ(G)$, then we have to show that G is abelian. For this let $x, y \in G$, then

$$xZ(G), yZ(G) \in \frac{G}{Z(G)}$$

$aZ(G)$ is the generator, so

$$xZ(G) = (aZ(G))^m = a^m Z(G)$$
$$\Rightarrow x(a^m)^{-1} Z(G) = Z(G)$$
$$\Rightarrow x(a^m)^{-1} \in Z(G)$$
$$\Rightarrow x(a^m)^{-1} = z, \quad z \in Z(G)$$
$$\Rightarrow x = za^m$$

$$yZ(G) = (aZ(G))^n = a^n Z(G)$$
$$\Rightarrow y(a^n)^{-1} Z(G) = Z(G)$$
$$\Rightarrow y(a^n)^{-1} \in Z(G)$$
$$\Rightarrow y(a^n)^{-1} = z', \quad z' \in Z(G)$$
$$\Rightarrow y = z'a^n$$

Now

$$xy = (za^m)(z'a^n)$$
$$= za^m z'a^n = zz'a^m a^n = zz'a^{m+n} = zz'a^{n+m}$$
$$= zz'a^n a^m = z'a^n za^m = (z'a^n)(za^m) = yx$$

This shows that G is an abelian group.

7-4 Automorphism Group of a Group

7-4.1 Definition:

An isomorphism from a group G to itself is called an *automorphism* of G.

In other words, a bijective homomorphism $\alpha : G \to G$ is called an *automorphism* of G.

The set of all automorphisms of a group G is called an *automorphism group* and is denoted by $A(G)$.

In the following theorem, we prove that $A(G)$ is a group.

7-4.2 Theorem:

The set $A(G)$ of all automorphisms of a group G is a group.

Proof:

G_1): Let $\alpha, \beta \in A(G)$, then $\alpha\beta$, being the product of two bijective mappings is bijective. To show that $\alpha\beta$ is a homomorphism, let

$$\begin{aligned}\alpha\beta(g_1g_2) &= \alpha(\beta(g_1g_2)) \\ &= \alpha(\beta(g_1)\beta(g_2)) \quad \because \beta \text{ is a homomorphi sm} \\ &= \alpha(\beta(g_1))\alpha(\beta(g_2)) \because \alpha \text{ is a homomorphi sm} \\ &= \alpha\beta(g_1)\alpha\beta(g_2)\end{aligned}$$

This shows that $\alpha\beta$ is a homomorphism, so $\alpha\beta \in A(G)$.

This shows that closure law holds in $A(G)$.

G_2): The associative law in $A(G)$ follows from the associativity of mapping of a set.

G_3): The identity mapping $I : G \to G$ defined by

$$I(g) = g, \qquad \forall g \in G$$

is a bijective mapping.

Next, using the definition of identity mapping, we have

$$\begin{aligned}I(g_1g_2) &= g_1g_2 \\ &= I(g_1)I(g_2)\end{aligned}$$

This shows that I is a homomorphism. Now I, being the bijective homomorphism, is in $A(G)$, i.e. $I \in A(G)$.

For any $\alpha \in A(G)$, we have

$$\alpha I(g) = \alpha(I(g)) = \alpha(g) \because I(g) = g$$

$$\Rightarrow \alpha I = \alpha$$

$$I\alpha(g) = I(\alpha(g)) = \alpha(g) \because I(\alpha(g)) = \alpha(g)$$

$$\Rightarrow I\alpha = \alpha$$

$$\Rightarrow \alpha I = \alpha = I\alpha$$

This shows that I is an identity element of $A(G)$, so identity law holds in $A(G)$.

G_4): For any $\alpha \in A(G)$, $\alpha^{-1}: G \to G$, being the inverse mapping of a bijective mapping, is bijective.

To show that α^{-1} is a homomorphism, let

$$\begin{aligned}
\alpha^{-1}(g_1g_2) &= \alpha^{-1}(I(g_1g_2)) && \because I(g_1g_2) = g_1g_2 \\
&= \alpha^{-1}(I(g_1)\cdot I(g_2)) && \because I \text{ is a homomorphi sm} \\
&= \alpha^{-1}(\alpha\alpha^{-1}(g_1)\cdot \alpha\alpha^{-1}(g_2)) && \because \alpha\alpha^{-1} = I \\
&= \alpha^{-1}(\alpha(\alpha^{-1}(g_1)\cdot \alpha^{-1}(g_2)) && \because \alpha \text{ is a homomorphi sm} \\
&= \alpha^{-1}\alpha(\alpha^{-1}(g_1)\cdot \alpha^{-1}(g_2)) \\
&= I(\alpha^{-1}(g_1)\cdot \alpha^{-1}(g_2)) \\
&= \alpha^{-1}(g_1)\cdot \alpha^{-1}(g_2)
\end{aligned}$$

This shows that α^{-1} is a homomorphism. Now α^{-1}, being the bijective homomorphism, is in $A(G)$, i.e. $\alpha^{-1} \in A(G)$.

This shows that α^{-1} is an inverse of α, so inverse of each element of $A(G)$ is in $A(G)$.

Since all the axioms of a group are satisfied, so $A(G)$ is a group.

7-4.3 Definition: Let a be a fixed element of a group G, then the mapping

$$I_a: G \to G$$

defined by

$$I_a(g) = aga^{-1}, \quad \forall g \in G$$

is called an *inner automorphism* from G to G.

Any other automorphism (if exits) is called an *outer automorphism.*

7-4.4 Example: *Let* $V_4 = \{e, a, b, ab\}$. *Find* $I_a: V_4 \to V_4$ *and show that* I_a *an inner automorphism from G to G.*

Solution: Let us define I_a by

$$I_a(g) = aga^{-1}, \quad \forall g \in V_4$$

Then

$$\begin{aligned}
I_a(e) &= a\cdot e\cdot a^{-1} = e \\
I_a(a) &= a\cdot a\cdot a^{-1} = a \\
I_a(b) &= a\cdot b\cdot a^{-1} = b \\
I_a(ab) &= a\cdot ab\cdot a^{-1} = ab
\end{aligned}$$

This shows that

$$I_a = \begin{pmatrix} e & a & b & ab \\ e & a & b & ab \end{pmatrix}$$

This shows that I_a is an identity mapping, so it is bijective mapping.

Next consider

$$\begin{aligned} I_a(g_1g_2) &= ag_1g_2a^{-1} \\ &= ag_1eg_2a^{-1} \\ &= ag_1a^{-1}ag_2a^{-1} \\ &= I_a(g_1)I_a(g_2) \end{aligned}$$

This shows that I_a is a homomorphism, so I_a is an inner automorphism.

7-4.5 Theorem:

The set $I(G)$ of all inner automorphisms of a group G is a normal subgroup of $A(G)$.

Proof: Let $I_a, I_b \in I(G)$, then

$$I_a(g) = aga^{-1}, \quad I_b(g) = bgb^{-1}, \quad \forall g \in A(G)$$

Next consider

$$\begin{aligned} I_aI_b^{-1}(g) &= I_a(I_{b^{-1}}(g)) \\ &= I_a(b^{-1}gb) \\ &= a(b^{-1}gb)a^{-1} \\ &= (ab^{-1})g(ba^{-1}) \\ &= (ab^{-1})g(ab^{-1})^{-1} \\ &= I_{ab^{-1}}(g) \in I(G) \end{aligned}$$

This shows that $I(G)$ is a subgroup of $A(G)$.

To prove that $I(G)$ is normal in $A(G)$, let $\alpha \in A(G)$, $I_a \in I(G)$ and consider

$$\begin{aligned} (\alpha I_a\alpha^{-1})(g) &= \alpha I_a(\alpha^{-1}(g)) \\ &= \alpha(a\alpha^{-1}(g)a^{-1}) \\ &= \alpha(a)\alpha\alpha^{-1}(g)\alpha(a^{-1}) \qquad \because \alpha \text{ is a homomorphi sm} \\ &= \alpha(a)(g)(\alpha(a))^{-1} \\ &= I_{\alpha(a)}(g) \in I(G) \end{aligned}$$

This shows that $I(G)$ is normal in $A(G)$.

7-4.6 Theorem:

Let G be a group, then $\dfrac{G}{Z(G)} \approx I(G)$.

PU, 2013 (M.Sc. Math)

Proof: To prove this theorem, we shall use first fundamental theorem of homomorphism.

Let us define a mapping

$$\phi : G \to I(G)$$

by $$\phi(g) = I_g, \qquad \forall g \in G$$

(i) Well defined

$$g_1 = g_2$$
$$\Rightarrow g_1^{-1} = g_2^{-1}$$
$$\Rightarrow g_1 g g_1^{-1} = g_2 g g_2^{-1}$$
$$\Rightarrow I_{g_1}(g) = I_{g_2}(g)$$
$$\Rightarrow \phi(g_1) = \phi(g_2)$$

This shows that ϕ is well defined.

(ii) Onto

For $I_g \in I(G)$, there is some $g \in G$ such that $\phi(g) = I_g$, so every element of $I(G)$ is an image of some element of G, so ϕ is onto.

(iii) Homomorphism

For $g_1, g_2 \in G$, we have

$$\begin{aligned}\phi(g_1 g_2) &= I_{g_1 g_2}(g)\\ &= g_1 g_2 \cdot g \cdot (g_1 g_2)^{-1}\\ &= g_1 g_2 \cdot g \cdot (g_2^{-1} g_1^{-1})\\ &= g_1 (g_2 g g_2^{-1}) g_1^{-1}\\ &= g_1 (I_{g_2}(g)) g_1^{-1}\\ &= I_{g_1}(I_{g_2})\\ &= \phi(g_1)\phi(g_2)\end{aligned}$$

This shows that ϕ is a homomorphism.

Thus, ϕ, being onto homomorphism, is an epimorphism.

Next we show that $Z(G) = K_\phi$, for this let

$$a \in K_\phi$$
$$\Rightarrow \phi(a) = I_e$$
$$\Rightarrow I_a = I_e \qquad \because \phi(a) = I_a$$
$$\Rightarrow I_a(g) = I_e(g) \qquad g \in G$$
$$\Rightarrow aga^{-1} = ege^{-1}$$
$$\Rightarrow aga^{-1} = g$$
$$\Rightarrow ag = ga \qquad \forall g \in G$$

$$\Rightarrow a \in Z(G)$$
$$\Rightarrow K_\phi \subseteq Z(G)$$

Conversely, let ...(1)

$$a \in Z(G)$$
$$\Rightarrow ag = ga \qquad \forall g \in G$$
$$\Rightarrow aga^{-1} = g$$
$$\Rightarrow aga^{-1} = ege^{-1}$$
$$\Rightarrow I_a(g) = I_e(g)$$
$$\Rightarrow I_a = I_e$$
$$\Rightarrow \phi(a) = I_e \qquad \because \phi(a) = I_a$$
$$\Rightarrow a \in K_\phi$$
$$\Rightarrow Z(G) \subseteq K_\phi \qquad ...(2)$$

Combining (1) and (2), we have

$$Z(G) = K_\phi$$

Using first fundamental theorem of homomorphism, we have

$$\frac{G}{Z(G)} \approx I(G)$$

This completes the proof.

7-4.7 Theorem:

Let G be a group. The mapping $\phi : G \to G$ defined by

$$\phi(g) = g^{-1}, \qquad g \in G$$

is an automorphism if and only if G is abelian.

Proof: Let the mapping $\phi : G \to G$ defined by

$$\phi(g) = g^{-1}, \qquad g \in G$$

is an automorphism, then we have to show that G is abelian.

Since ϕ is automorphism, so for $g_1, g_2 \in G$

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$
$$= g_1^{-1} g_2^{-1}$$

But
$$\phi(g_1 g_2) = (g_1 g_2)^{-1}$$
$$= g_2^{-1} g_1^{-1}$$

Therefore

$$g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1}$$
$$\Rightarrow (g_1 g_2)^{-1} = (g_2 g_1)^{-1}$$
$$\Rightarrow g_1 g_2 = g_2 g_1 \qquad \forall g_1, g_2 \in G$$

This shows that g is an abelian group.

Conversely, let G be abelian group and consider a mapping $\phi: G \to G$ defined by

$$\phi(g) = g^{-1}, \qquad g \in G$$

(i) Well defined

$$g_1 = g_2$$
$$\Rightarrow g_1^{-1} = g_2^{-1}$$
$$\Rightarrow \phi(g_1) = \phi(g_2)$$

This shows that ϕ is well defined.

(ii) One-one

$$\phi(g_1) = \phi(g_2)$$
$$\Rightarrow g_1^{-1} = g_2^{-1}$$
$$\Rightarrow g_1 = g_2$$

This shows that ϕ is one-one.

(iii) Onto

For $g^{-1} \in G$, there is some $g \in G$ such that $\phi(g) = g^{-1}$, so every element of G is an image of some element of G, so ϕ is onto.

(iv) Homomorphism

For $g_1, g_2 \in G$, we have

$$\phi(g_1 g_2) = (g_1 g_2)^{-1}$$
$$= g_2^{-1} g_1^{-1}$$
$$= g_1^{-1} g_2^{-1} \qquad \because G \text{ is abelian}$$
$$= \phi(g_1)\phi(g_2)$$

This shows that ϕ is a homomorphism, so ϕ is an automorphism.
This completes the proof.

7-4.8 Theorem: *Let G be a group which has an element of order > 2. Then G has an automorphism different from the identity automorphism.*

Proof: If G an abelian group, then (by previous theorem) a mapping $\phi: G \to G$ defined by

$$\phi(g) = g^{-1}, \qquad g \in G$$

is an automorphism different from identity automorphism.

If G is a non-abelian group and contains an element of order > 2, then there is $g \in G$ such that $ag \neq ga$.

Then the mapping

$$I_g(a) = gag^1 \neq a$$

is an automorphism different from identity automorphism.
This completes the proof.

7-5 Commutator Subgroups of a Group

7-5.1 Definition:

Let G be a group and $a,b \in G$, then the element $aba^{-1}b^{-1}$ is called the *commutator* of a and b. It is denoted by $[a,b]$, i.e.

$$[a,b] = aba^{-1}b^{-1}$$

7-5.2 Example: *Prove the following commutator identities in a group G:*

(i) $[a,b]^{-1} = [b,a]$ (ii) $[ab,c] = [b,c]^a[a,c]$

(iii) $[a,bc] = [a,b][a,c]^b$ (iv) $[a,b^{-1}] = [b,a]^{b^{-1}}$

(v) $[a^{-1},b] = [b,a]^{a^{-1}}$

Solution: (i) Using the definition of commutator of a and b, we have

$$\begin{aligned}[a,b]^{-1} &= (aba^{-1}b^{-1})^{-1}\\ &= (b^{-1})^{-1}(a^{-1})^{-1}b^{-1}a^{-1}\\ &= bab^{-1}a^{-1}\\ &= [b,a]\end{aligned}$$

(ii) Using the definition of commutator of ab and c, we have

$$\begin{aligned}[ab,c] &= (ab)c(ab)^{-1}c^{-1}\\ &= abc(b^{-1}a^{-1})c^{-1}\\ &= abcb^{-1}a^{-1}c^{-1}\\ &= abcb^{-1}ea^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}ca^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}eca^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1}\\ &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1})\\ &= a[b,c]a^{-1}[a,c]\\ &= [b,c]^a[a,c] \qquad \because axa^{-1} = x^a\end{aligned}$$

We can also prove alternatively, taking right hand side as follows:

$$\begin{aligned}[b,c]^a[a,c] &= a[b,c]a^{-1}[a,c] \qquad \because axa^{-1} = x^a\\ &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1})\\ &= abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}eca^{-1}c^{-1} \qquad \because a^{-1}a = e\\ &= abcb^{-1}c^{-1}ca^{-1}c^{-1}\\ &= abcb^{-1}ea^{-1}c^{-1} \qquad \because c^{-1}c = e\end{aligned}$$

$$[b,c]^a[a,c] = abcb^{-1}a^{-1}c^{-1}$$
$$= abc(ab)^{-1}c^{-1}$$
$$= [ab,c]$$

(iii) Using the definition of commutator of elements, we have

$$[a,b][a,c]^b = [a,b]b[a,c]b^{-1} \quad \because [a,c]^b = b[a,c]b^{-1}$$
$$= (aba^{-1}b^{-1})b(aca^{-1}c^{-1})b^{-1}$$
$$= aba^{-1}(b^{-1}b)aca^{-1}c^{-1}b^{-1}$$
$$= aba^{-1}eaca^{-1}c^{-1}b^{-1} \quad \because b^{-1}b = e$$
$$= aba^{-1}aca^{-1}c^{-1}b^{-1}$$
$$= abeca^{-1}c^{-1}b^{-1} \quad \because a^{-1}a = e$$
$$= abca^{-1}c^{-1}b^{-1}$$
$$= abca^{-1}(bc)^{-1}$$
$$= [a,bc]$$

(iv) Using the definition of commutator of elements, we have

$$[b,a]^{b^{-1}} = b^{-1}[b,a](b^{-1})^{-1}$$
$$= b^{-1}[b,a]b$$
$$= b^{-1}(bab^{-1}a^{-1})b$$
$$= b^{-1}bab^{-1}a^{-1}b$$
$$= eab^{-1}a^{-1}b \quad \because b^{-1}b = e$$
$$= ab^{-1}a^{-1}b$$
$$= ab^{-1}a^{-1}(b^{-1})^{-1}$$
$$= [a,b^{-1}]$$

(v) Using the definition of commutator of elements, we have

$$[b,a]^{a^{-1}} = a^{-1}[b,a](a^{-1})^{-1}$$
$$= a^{-1}[b,a]a$$
$$= a^{-1}(bab^{-1}a^{-1})a$$
$$= a^{-1}bab^{-1}a^{-1}a$$
$$= a^{-1}bab^{-1}e$$
$$= a^{-1}bab^{-1}$$
$$= a^{-1}b(a^{-1})^{-1}b^{-1}$$
$$= [a^{-1},b]$$

7-5.3 Definition:

Let G be a group. The set of all commutators $[a,b]$ of $a,b \in G$ is called the *first derived subgroup* of G and is denoted by

$$G^{(1)} = [G, G]$$

The set of all commutators of a group $G^{(1)}$ is called the *first derived subgroup* of $G^{(1)}$ and the *second derived subgroup* of G. It is denoted by

$$G^{(2)} = [G^{(1)}, G^{(1)}]$$

Similarly

$$G^{(3)} = [G^{(2)}, G^{(2)}]$$
$$\vdots \qquad \vdots$$
$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$$

7-5.4 Theorem:

Let G be a group, then the derived group $G^{(1)}$ is a normal subgroup of G.

Proof:

Let $a,b \in G$, then $[a,b] \in G^{(1)} = [G, G]$.

For any $g \in G$, consider

$$\begin{aligned} g[a,b]g^{-1} &= g(aba^{-1}b^{-1})g^{-1} \quad \because [a,b] = aba^{-1}b^{-1} \\ &= gaba^{-1}b^{-1}g^{-1} \\ &= gaebea^{-1}eb^{-1}g^{-1} \\ &= gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} \\ &= a^g b^g (a^{-1})^g (b^{-1})^g \\ &= a^g b^g (a^g)^{-1}(b^g)^{-1} \\ &= [a^g, b^g] \end{aligned}$$

$$\Rightarrow g[a,b]g^{-1} \in G^{(1)} \qquad \because [a^g, b^g] \in G^{(1)}$$

This shows that $G^{(1)}$ is a normal subgroup of G.

EXERCISE 7

Short Questions

Q.1 Solve / answer the following short questions:

(i) If H is a normal subgroup of G then show that $g^{-1}Hg = H$ for all $g \in G$.

(ii) If $g^{-1}Hg = H$ for all $g \in G$, then show that H is a normal subgroup of G.

(iii) Show that every subgroup of an abelian group is its normal subgroup.

(iv) If H is a subgroup of a group G then show that $HH = H$.

(v) Show that the intersection of two normal subgroups of G is a normal subgroup of G.

(vi) If H is a subgroup of a group G, then show that H is a normal subgroup of $N_G(H)$.

(vii) Define factor group.

(viii) If $V_4 = \{e, a, b, ab\}$ and $N = \{e, a\}$ the normal subgroup of V_4. Find the quotient group $\frac{V_4}{N}$.

(ix) Define automorphism.

(x) Define the commutator of a and b in a group G.

Long Questions

Q.2 Show that the subgroup H of G is a normal subgroup of G if and only if every left coset of H in G is a right coset of H in G.

Q.3 If G is a group and H is a subgroup of index 2 in G, then show that H is a normal subgroup of G.

PU, 2008 (M.Sc. Math)

Q.4 If H and K are two normal subgroups of a group G such that $H \cap K = \{e\}$, then show that $hk = kh$ for all $h \in H, k \in K$.

PU, 2009; 2003 (M.Sc. Math)

Q.5 If a cyclic subgroup K of G is normal in G then show that every subgroup of K is normal in G.

Q.6 If H and K are normal subgroups of a group G, then prove that HK is a normal subgroup of G.

PU, 2008; 2005; 2000 (M.Sc. Math)

Q.7 Let G and G' be two groups. Let $\phi : G \to G'$ be an epimorphism, then $\frac{G}{K_\phi} \approx G'$.

PU, 2010 (M.Sc. Math)

SUMMARY

- A subgroup H of a group G is said to be self conjugate or normal subgroup of G if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.
- A subgroup H of a group G is said to be normal subgroup of G if $g^{-1}Hg \subset H$ for all $g \in G$.
- H is a normal subgroup of G if and only if $gHg^{-1} = H$ for all $g \in G$.
- Every subgroup of an abelian group is its normal subgroup.
- The subgroup H of G is a normal subgroup of G if and only if every left coset of H in G is a right coset of H in G.
- If H is a subgroup of a group G then $HH = H$.
- A subgroup H of G is a normal subgroup of G if and only if the product of two right cosets of H in G is again a right coset of H in G.
- A subgroup of index 2 is normal subgroup.
- The intersection of two normal subgroups is normal.
- The intersection of any number of normal subgroups is normal.
- If a cyclic subgroup K of G is normal in G then every subgroup of K is normal in G.
- If H and K are normal subgroups of a group G, then HK is a normal subgroup of G.
- If H is a subgroup of a group G, then H is a normal subgroup of $N_G(H)$.
- The centralizer of a normal subgroup H of a group G is normal in G.
- If N is a normal subgroup of a group G, then $\frac{G}{N}$ is called quotient or factor group.
- Let G and G' be two groups and $\phi : G \to G'$ is a homomorphism then kernel of homomorphism is a normal subgroup of G.
- An isomorphism from a group G to itself is called an automorphism of G.

- The set of all automorphisms of a group G is called an automorphism group and is denoted by $A(G)$.
- The set $I(G)$ of all inner automorphisms of a group G is a normal subgroup of $A(G)$.
- Let G be a group which has an element of order > 2. Then G has an automorphism different from the identity automorphism.
- Let G be a group and $a,b \in G$, then the element $aba^{-1}b^{-1}$ is called the commutator of a and b.
- Let G be a group. The set of all commutators $[a,b]$ of $a,b \in G$ is called the first derived subgroup.
- Let G be a group, then the derived group $G^{(1)}$ is a normal subgroup of G.

*****

Chapter

8

SYLOW THEOREMS

8-1 Cauchy's Theorems for Abelian and Non-Abelian Groups

8-1.1 Cauchy's Theorem for Abelian Group:

If A is a finite abelian group and p a prime divisor of the order of A, then A contains an element of order p.

PU, 2013 (M.Sc. Math)

Proof: Let A be an abelian group of order n and p a prime divisor of n. We will prove the theorem using induction on the order of A.

If $n = p$, then A is cyclic group of order p and the order of generator of A is p, so we have a basis for induction.

Suppose that the theorem is true for all abelian groups of order less than n and divisible by p.

Consider now a group A. Let $a \neq 1$ be an element of A and H and H is the cyclic group generated by a, then there are following two possibilities:

(i) The order k of H is divisible by p.

(ii) The order k of H is not divisible by p.

Case (i) If order k of H is divisible by p, then

$$k = pq, \quad q \geq 1$$

$$\Rightarrow a^k = a^{pq} = (a^q)^p = 1$$

This shows that a^q is an element of order p in H and so in G.

Case (ii) If order k of H is not divisible by p.

Since A is abelian, so H is normal in A. Therefore, $\frac{A}{H}$ is a factor group having order less than n but divisible by p, so by our assumption $\frac{A}{H}$ has an element of order p, i.e.

$$(xH)^p = H, \quad x \in A$$
$$\Rightarrow x^p H = H$$
$$\Rightarrow x^p \in H$$

As $(p,k)=1$, so x^p also generates H, i.e.

$$(x^p)^k = (x^k)^p = 1$$

This shows that x^k has order p and $x^k \in H$, so $x^k \in G$.
This completes the proof.

8-1.2 Cauchy's Theorem for Non-Abelian Group:

If a prime p divides the order of a group G then G contains an element of order p.

Proof: Let G be a group of order n divisible by p. We will prove the theorem by using induction on the order of G. If $n = p$, then G is a cyclic group of order p and the order of its generator is p, so we have a basis for induction.

Suppose that the theorem is true for all groups of order less than n and divisible by p.

Now we have the following possibilities:

(i) G contains a proper subgroup whose order is divisible by p (index is prime to p).

(ii) Every proper subgroup H of G has index divisible by p.

Case (i) Since order of G is les than order of G and is divisible by p, so H has an element of order p (by assumption) which is an element of order p of G.

Case (ii) We know that the centre of p-group is nontrivial.

Let the class equation of G be

$$n = n_1 + n_2 + \ldots + n_k \qquad \ldots(1)$$

Where n_i is the number of elements in a conjugacy class in G. Now each n_i, being the index of the normalizer in the ith conjugacy class, is divisible by p (by (ii))

Since identity is self conjugate, so without any loss of generality, suppose that $n_1 = 1$. Using this in (1), we have

$$n = 1 + n_2 + \ldots + n_k$$
$$1 = n - (n_2 + \ldots + n_k) \qquad \ldots(2)$$

Right hand side of (2) is divisible by p, so its left hand side should also be divisible by p.

But $n_1 = 1$, so the number of n_i's which are equal to one must be p or multiple of p. The corresponding conjugacy classes, i.e. for which $n_i = 1$ are such that each consists of central element.

Hence the order of $Z(G)$ is a multiple of p. Since $Z(G)$ is always abelian and its order is divisible by p, so by Cauchy's theorem for abelian group, $Z(G)$ has an element of order p in G which is also an element of order p in G.

This completes the proof.

8-2 Sylow's Theorems

8-2.1 Definition (p-Group): A group G is said to be a *p-group* if the order of every element of G can be written as p^α, for some fixed p.

For example, consider the elements of $V_4 = \{e, a, b, ab\}$ group.

Since

$$o(e) = 1 = 2^0, \qquad o(a) = 2 = 2^1,$$
$$o(b) = 2 = 2^1, \qquad o(ab) = 2 = 2^1$$

This shows that the order of every element of V_4 can be written as 2^α, for 2, so V_4 is a p-group, with $p = 2$.

8-2.2 Definition (Sylow p-Subgroup): Let G be a group of order n and p a prime divisor of n. Subgroup H of G is said to be a *sylow p-subgroup* of G if H has order p^α, where p^α divides n and no other power of p divides n.

8-2.3 Theorem (Sylow's First Theorem):

A finite group whose order is divisible by a prime p, contains a sylow p-subgroup.

PU, 2011; 2008 (M.Sc. Math)

Proof: Let G be a group of order n and p a prime divisor of order n. To prove the theorem, we apply induction on the order of G.

If $n = p$, then G itself is a p-subgroup and nothing is to prove.

Suppose that the theorem is true for all groups of order less than n and divisible by p. We have the following two possibilities:

(i) There is a subgroup H of G with index prime to p.

(ii) Every subgroup H of G has index divisible by p.

Case (i) If H has order less than n and divisible by p, then by supposition, H has a sylow p-subgroup.

Since index is prime to p, therefore, the sylow p-subgroup of H is a sylow p-subgroup of G.

Case (ii) $Z(G)$ is nontrivial and the order of $Z(G)$ is multiple of p. By Cauchy's theorem, $Z(G)$ contains an element of order p, so

$$C = < z : z^p = 1 >$$

Then C is a subgroup of $Z(G)$ and is normal in G, so the quotient group $\frac{G}{C}$ is well defined. The order of $\frac{G}{C}$ is less than the order of G and is divisible by $p^{\alpha-1}$ and no higher power of p.

Therefore, by assumption, $\frac{G}{C}$ has a sylow p-subgroup say $\frac{H}{C}$ of order $p^{\alpha-1}$, where H is a subgroup of G. The order of H is then

$$\left|\frac{H}{C}\right| = p^{\alpha-1}$$

$$|H| = |C|p^{\alpha-1}$$

$$|H| = pp^{\alpha-1}$$

$$|H| = p^{\alpha}$$

This shows that H is a sylow p-subgroup of G.
Hence, a finite group whose order is divisible by a prime p, contains a sylow p-subgroup.

This completes the proof.

8-2.4 Theorem (Sylow's Second Theorem):

Any two sylow p-subgroups of a group are conjugate. PU, 2009 (M.Sc. Math)

Proof: Let G be a group of order n
Let H, K be any two sylow p-subgroups of order p^{α} in G, then

$$n = p^{\alpha}m, \qquad (p,m) = 1$$

Consider the double coset representation of G module (H,K)

$$G = \bigcup_{i=1}^{r} Ha_iK, \quad a_i \in G$$

Then

$$n = \sum_{i=1}^{r} \frac{p^{\alpha}p^{\alpha}}{q_i} \qquad ...(1)$$

Where q_i is the order of $H \cap a_iKa_i^{-1}$.

Dividing both sides of (1) by p^{α}, we have

$$m = \frac{n}{p^\alpha} = \sum_{i=1}^{r} \frac{p^\alpha}{q_i}$$

$$m = \sum_{i=1}^{r} \frac{p^\alpha}{q_i} \qquad ...(2)$$

Now q_i, being the order of intersection of two p-groups, is a multiple of p, so each term of the right hand side of (2) is either a multiple of p or equal to 1.

Since the left hand side of (2) is not divisible by p, so at least one

$$\frac{p^\alpha}{q_i} = 1, \qquad i = 1,2,...,r$$

Without any loss of generality, let

$$\frac{p^\alpha}{q_1} = 1$$

or $$p^\alpha = q_1$$

So that the order of $H \cap a_i K a_i^{-1}$ is p^α.

But $H \cap a_i K a_i^{-1}$, being the subgroup of H having order same as H, divides with H, i.e.

$$H \cap a_i K a_i^{-1} = K$$

$$\Rightarrow H \subseteq H \cap a_i K a_i^{-1}, \quad a_i \in G$$

As the order of H is same as the order of $a_i K a_i^{-1}$, so

$$H = a_i K a_i^{-1}, \quad a_i \in G$$

This shows that H and K are conjugate.
Hence, any two sylow p-subgroups of a group are conjugate.
This completes the proof.

8-2.5 Theorem:

A finite group G has a unique sylow p-subgroup H if and only if H is normal in G.

PU, 2013 (M.Sc. Math)

Proof: Let H be a unique sylow p-subgroup of finite group G. Let $a \in G$, then aHa^{-1} is a sylow p-subgroup of G.

$$H = aHa^{-1}$$

$$\Rightarrow H \triangleleft G$$

This shows that H is normal in G.

Conversely, suppose that H is normal in G, then

$$H = aHa^{-1} \qquad \forall a \in G$$

Since all sylow p-subgroups of G are of the form aHa^{-1}, and all these coincide with H, so H is a unique sylow p-subgroup.

8-2.6 Theorem (Sylow's Third Theorem):

The number k of sylow p-subgroups of a finite group is congruent to 1 mod p and is a factor of the order of the group.

PU, 2012 (M.Sc. Math)

Proof: Let H be a sylow p-subgroup of a finite group G. Let n be the order of G. Since any two sylow p-subgroups are conjugate, so the number of sylow p-subgroups of G is equal to the number of subgroups in the conjugacy class of H and this is same as the index of the normalizer

$$N_G(H) = N \quad \text{(say)}$$

Let $|H| = p^\alpha$, $|N| = n$ and its index be k. We have to show that

$$k = 1 \bmod p$$

Consider the double coset decomposition modulo (N,H) of G.

$$G = \bigcup_{i=1}^{r} Na_iH, \quad a_i \in G$$

Then

$$n = \sum_{i=1}^{r} \frac{n_i p^\alpha}{q_i}$$

Where q_i is the order of $N \cap a_iHa_i^{-1}$ so is a power of p because it is the order of a subgroup of p-group. Hence

$$k = \sum_{i=1}^{r} \frac{p^\alpha}{q_i} \qquad \ldots(1)$$

Where k is the order of N in G. Each term on the right hand side of (1) is a multiple of p or equal to 1. However, one of the terms among the double coset Na_1H (say), is such that for $a_1 = e$

$$Na_1H = NH = N$$

And $N \cap H = H$

Therefore, $q_1 = p^\alpha$

Putting this in (1), we have

$$k = 1 + \sum_{i=2}^{r} \frac{p^\alpha}{q_i} \qquad \ldots(2)$$

This shows that no term on the right hand side of (2) is unity.

Suppose on contrary that for some $j > 1$, $\frac{p^\alpha}{q_j} = 1$, i.e. $q_j = p^\alpha$. Then the intersection $N \cap a_jHa_j^{-1}$, being the subgroup of $a_jHa_j^{-1}$ having order equal to the order of $a_jHa_j^{-1}$, must coincide with $a_jHa_j^{-1}$, so

$$a_jHa_j^{-1} = N \cap a_jHa_j^{-1}$$

$$\Rightarrow a_jHa_j^{-1} \subseteq N$$

Since a sylow p-subgroup H of G is a sylow p-subgroup of any subgroup containing H, H is a sylow p-subgroup of N. But H is normal in G, so H is unique sylow p-subgroup of N, so

$$H = a_j H a_j^{-1}$$

Then $a_j \in N$, so

$$Na_jH = NH = N$$

This gives $j = 1$ which is a contradiction.

This completes the proof.

SUMMARY

- If A is a finite abelian group and p a prime divisor of the order of A, then A contains an element of order p.
- If a prime p divides the order of a group G then G contains an element of order p.
- A group G is said to be a p-group if the order of every element of G can be written as p^α, for some fixed p.
- Let G be a group of order n and p a prime divisor of n. Subgroup H of G is said to be a sylow p-subgroup of G if H has order p^α, where p^α divides n and no other power of p divides n.
- A finite group whose order is divisible by a prime p, contains a sylow p-subgroup.
- Any two sylow p-subgroups of a group are conjugate.
- A finite group G has a unique sylow p-subgroup H if and only if H is normal in G.
- The number k of sylow p-subgroups of a finite group is congruent to 1 mod p and is a factor of the order of the group.

*****

ANSWERS

EXERCISE 1

Multiple Choice Questions (MCQs)

Q.1

(i)	●	b	c	d	(ii)	a	●	c	d
(iii)	a	b	c	●	(iv)	a	b	●	d
(v)	a	b	c	●	(vi)	a	b	●	d
(vii)	a	●	c	d	(viii)	a	●	c	d
(ix)	●	b	c	d	(x)	a	b	●	d
(xi)	a	●	c	d	(xii)	a	b	●	d
(xiii)	a	b	c	●	(xiv)	a	b	c	●
(xv)	a	●	c	d	(xvi)	a	b	●	d
(xvii)	a	b	c	●	(xviii)	●	b	c	d
(xix)	a	b	c	●	(xx)	●	b	c	d

EXERCISE 2

Multiple Choice Questions (MCQs)

Q.1

(i)	a	●	c	d	(ii)	a	b	●	d
(iii)	a	b	●	d	(iv)	●	b	c	d
(v)	a	b	c	●	(vi)	a	b	●	d
(vii)	a	b	●	d	(viii)	a	●	c	d
(ix)	●	b	c	d	(x)	a	b	c	●
(xi)	a	●	c	d	(xii)	●	b	c	d
(xiii)	a	●	c	d	(xiv)	a	●	c	d
(xv)	a	●	c	d	(xvi)	a	b	●	d
(xvii)	a	b	c	●	(xviii)	●	b	c	d
(xix)	a	b	c	●	(xx)	●	b	c	d

Q.2

(i)	a	b	●	d	(ii)	a	b	●	d
(iii)	●	b	c	d	(iv)	a	b	c	●
(v)	a	b	c	●	(vi)	a	b	●	d
(vii)	a	b	●	d	(viii)	●	b	c	d
(ix)	a	b	c	●	(x)	●	b	c	d
(xi)	a	b	c	●	(xii)	a	●	c	d
(xiii)	a	●	c	d	(xiv)	a	b	c	●
(xv)	●	b	c	d	(xvi)	a	b	c	●
(xvii)	a	b	c	●	(xviii)	a	b	●	d
(xix)	a	b	c	●	(xx)	●	b	c	d

Q.3

(i)	●	b	c	d	(ii)	●	b	c	d
(iii)	●	b	c	d	(iv)	●	b	c	d
(v)	a	●	c	d	(vi)	a	●	c	d
(vii)	a	●	c	d	(viii)	a	●	c	d
(ix)	a	●	c	d	(x)	a	●	c	d
(xi)	a	●	c	d	(xii)	a	b	●	d
(xiii)	a	b	●	d	(xiv)	a	b	c	●
(xv)	a	b	●	d	(xvi)	●	b	c	d
(xvii)	a	●	c	d	(xviii)	●	b	c	d
(xix)	a	●	c	d	(xx)	a	b	●	d

Q.4

(i)	a	b	●	d	(ii)	a	●	c	d
(iii)	a	●	c	d	(iv)	a	b	c	●
(v)	●	b	c	d	(vi)	a	●	c	d
(vii)	a	b	●	d	(viii)	a	b	c	●
(ix)	a	b	c	●	(x)	a	●	c	d

(xi) ⓐ ⓑ ⓒ ●
(xii) ⓐ ⓑ ⓒ ●
(xiii) ⓐ ⓑ ● ⓓ
(xiv) ⓐ ⓑ ● ⓓ
(xv) ⓐ ⓑ ⓒ ●
(xvi) ⓐ ⓑ ⓒ ●
(xvii) ⓐ ⓑ ● ⓓ
(xviii) ⓐ ● ⓒ ⓓ
(xix) ⓐ ⓑ ● ⓓ
(xx) ● ⓑ ⓒ ⓓ

Q.5

(i) ⓐ ● ⓒ ⓓ
(ii) ⓐ ⓑ ⓒ ●
(iii) ⓐ ⓑ ⓒ ●
(iv) ⓐ ⓑ ● ⓓ
(v) ⓐ ● ⓒ ⓓ
(vi) ⓐ ⓑ ● ⓓ
(vii) ⓐ ⓑ ⓒ ●
(viii) ⓐ ⓑ ● ⓓ
(ix) ⓐ ● ⓒ ⓓ
(x) ⓐ ⓑ ● ⓓ
(xi) ● ⓑ ⓒ ⓓ
(xii) ⓐ ⓑ ● ⓓ
(xiii) ● ⓑ ⓒ ⓓ
(xiv) ⓐ ● ⓒ ⓓ
(xv) ⓐ ⓑ ● ⓓ
(xvi) ● ⓑ ⓒ ⓓ
(xvii) ⓐ ⓑ ⓒ ●
(xviii) ⓐ ● ⓒ ⓓ
(xix) ⓐ ● ⓒ ⓓ
(xx) ⓐ ⓑ ● ⓓ

EXERCISE 3

Multiple Choice Questions (MCQs)

Q.1

(i) ⓐ ⓑ ● ⓓ
(ii) ● ⓑ ⓒ ⓓ
(iii) ⓐ ⓑ ● ⓓ
(iv) ⓐ ⓑ ⓒ ●
(v) ⓐ ⓑ ⓒ ●
(vi) ⓐ ⓑ ⓒ ●
(vii) ⓐ ⓑ ● ⓓ
(viii) ⓐ ⓑ ● ⓓ
(ix) ● ⓑ ⓒ ⓓ
(x) ● ⓑ ⓒ ⓓ
(xi) ⓐ ⓑ ● ⓓ
(xii) ⓐ ● ⓒ ⓓ
(xiii) ⓐ ⓑ ⓒ ●
(xiv) ⓐ ● ⓒ ⓓ

EXERCISE 4

Multiple Choice Questions (MCQs)

Q.1

(i) ⓐ ⓑ ⓒ ● (ii) ⓐ ⓑ ● ⓓ

(iii) ⓐ ● ⓒ ⓓ (iv) ● ⓑ ⓒ ⓓ

(v) ⓐ ● ⓒ ⓓ (vi) ⓐ ⓑ ● ⓓ

(vii) ⓐ ⓑ ● ⓓ

EXERCISE 5

Multiple Choice Questions (MCQs)

Q.1

(i) ⓐ ● ⓒ ⓓ (ii) ⓐ ⓑ ● ⓓ

(iii) ⓐ ⓑ ⓒ ● (iv) ● ⓑ ⓒ ⓓ

(v) ⓐ ● ⓒ ⓓ (vi) ⓐ ⓑ ● ⓓ

(vii) ● ⓑ ⓒ ⓓ (viii) ⓐ ● ⓒ ⓓ

(ix) ⓐ ⓑ ● ⓓ (x) ⓐ ⓑ ● ⓓ

(xi) ⓐ ⓑ ● ⓓ (xii) ⓐ ⓑ ● ⓓ

EXERCISE 6

Multiple Choice Questions (MCQs)

Q.1

(i) ⓐ ● ⓒ ⓓ (ii) ⓐ ⓑ ⓒ ●

(iii) ⓐ ● ⓒ ⓓ (iv) ⓐ ⓑ ● ⓓ

(v) ⓐ ● ⓒ ⓓ (vi) ● ⓑ ⓒ ⓓ

(vii) ⓐ ⓑ ⓒ ● (viii) ⓐ ⓑ ● ⓓ

(ix) ⓐ ⓑ ⓒ ● (x) ⓐ ● ⓒ ⓓ

GLOSSARY

Abelian Group
The group $(G,*)$ is said to be an abelian group or commutative group if $a*b=b*a \quad \forall a,b \in G$.

Anti-symmetric Relation
The relation R on A is said to be anti-symmetric relation if $R \cap R^{-1} = I$.

Associative Law
A binary operation $*$ is said to satisfy the associative law in X if $x*(y*z)=(x*y)*z \qquad \forall x,y,z \in X$

Automorphism
An isomorphism from a group G to itself is called an automorphism of G.

Automorphism Group
The set of all automorphisms of a group G is called an automorphism group and is denoted by $A(G)$.

Binary Operation
Any mapping $*$ of $X \times X$ into X, where X is any nonempty set, is called a binary operation in X.

Binary Relation
A subset R of $A \times B$ is called a binary relation or simply a relation from A to B.

Bijective Mapping
If a mapping $f: X \to Y$ is both one-to-one and onto, we call f a one-to-one mapping of X onto Y. Such a mapping is also called the bijective mapping.

Cartesian Product
Let A and B be two nonempty sets, then the set consisting of all ordered pairs (a, b), where $a \in A$ and $b \in B$, is called the Cartesian product of A and B and is denoted by $A \times B$.

Cauchy's Theorem for Abelian Group
If A is a finite abelian group and p a prime divisor of the order of A, then A contains an element of order p.

Cauchy's Theorem for Non-Abelian Group
If a prime p divides the order of a group G then G contains an element of order p.

Centre of a Group
Centre of a group G is defined as $Z(G)=\{z \in G : zx = xz \forall x \in G\}$.

Centralizer
$N(a)=\{x \in G : xa = ax\}$ is normalizer or centralizer of a in G.

Centralizer of a Complex
Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with the elements of X is called centralizer of X in G and is denoted by $C_G(X)$.

Commutative Group
The group $(G,*)$ is said to be an abelian group or commutative group if $a*b=b*a \quad \forall a,b \in G$.

Commutative Law
A binary operation $*$ is said to satisfy the commutative law in X if $x*y=y*x \quad \forall x,y \in X$

Complement of a Relation
If R is a relation in A, then the complement of relation R is denoted by R^c and is defined as $R^c = (A \times A) - R$.

Complement of a Set
If $B \subset A$, then $A-B=\{x \in A : x \notin B\}$ is said to be the complement of B in A.

Composition of Permutations
If $f: X \to X$ and $g: X \to X$ are two permutations on a nonempty set X, then the permutation $fg: X \to X$ on X defined as $(x)fg=((x)f)g \quad \forall x \in X$ is called the product or composition of permutations f and g.

Commutator of Elements
If G is a group and $x,y \in G$, $x^{-1}y^{-1}xy$ is called the commutator of x and y or, more briefly, a commutator.

Conjugate Class
Set of all those elements of a group G which are conjugate of a in G is called conjugate class of a in G. It is denoted by $C(a)$.

Conjugate Elements
If b is a conjugate of a, then we say that a and b are conjugate elements.

Conjugate of an Element
If $a,b \in G$, then b is said to be a conjugate of a in G if there exists an element $g \in G$ such that $b=g^{-1}ag$.

Conjugate Subgroup
Let H be a subgroup of a group G, then for $g \in G$, gHg^{-1} is called conjugate subgroup of H.

Constant Function
A function whose range consists of just one element is called a constant function.

Complex in a Group An arbitrary subset X of a group G is said to be a complex in G.

Cyclic Group (multiplication) A group G is said to be cyclic group under multiplication if each element of G is a power of one and the same element of G. Such an element of the group is called the generator of the group.

Cyclic Group (addition) A group G is said to be a cyclic group under addition generated by a if each element of G is a multiple of a.

Degree of permutation If X is a finite set having n elements and f is a permutation on X, then n is called the degree of permutation f.

Descriptive Method A set can be expressed by descriptive statement and this way of expressing a set is called the descriptive method.

Difference of two Sets The difference $A-B$ of two sets A and B is defined to be set of those elements of A which are not in B.

Disjoint Sets Two sets A and B are said to be disjoint if they have no common points.

Double Coset Let H, K be two subgroups of a group G and $a \in G$, then HaK is called the double coset in G modulo (H,K) determined by a.

Embedding By embedding G into G', we mean that there is a subgroup of G' which is isomorphic to G.

Empty Relation A relation R from A to B is said to be empty or nullary if $R = \phi$.

Empty Set A set which contains no elements is called an empty set. It is denoted by ϕ.

Endomorphism A homomorphism from a group G to itself is called an endomorphism of G.

Epimorphism An onto homomorphism is called an epimorphism.

Equal Mappings The mappings f and g of X into Y are said to be equal if $f(x) = g(x)$ for every $x \in X$.

Equal Sets Two sets A and B are said to be equal if both are subsets of each other.

Equivalence Relation A relation R on a set A is called an equivalence relation if and only if R is reflexive, symmetric, and transitive.

Even Permutation
A permutation f in S_n is said to be an even permutation if it can be written as a product of an even number of transpositions.

Extension of a Function
A function f is called an extension of a function g if the domain of f contains the domain of g and $f(x) = g(x)$ for each x in the domain of g.

First Derived Subgroup
Let G be a group. The set of all commutators $[a,b]$ of $a,b \in G$ is called the first derived subgroup.

Function
Let X and Y be two nonempty sets. A rule f which assigns to each element x in X a single element y in Y is called a function.

Group
The nonempty set G is said to be group with respect to $*$ if for all $a,b,c \in G$,
(i) $a*b \in G$ (ii) $a*(b*c) = (a*b)*c$
(iii) there exists an element $e \in G$, such that $a*e = e*a = a$.
(iv) there exists an element $a' \in G$, such that $a*a' = a'*a = e$.

Homomorphism
A mapping ϕ from a group G into a group G' is said to be a homomorphism if for all $a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Idempotent
An element a of a group G is said to be idempotent if $a^2 = a$.

Identity Element
Let $*$ be a binary operation in a nonempty set X then an element $e \in X$ is said to be the identity element (with respect to $*$) of X if $e*x = x*e = x \; \forall x \in X$.

Identity Permutation
Let X be a nonempty set. A permutation $I : X \to X$ is said to be the identity permutation on X if $I(x) = x \quad \forall x \in X$.

Identity Relation
A binary relation I is called the identity relation on A if $I = \{(a, a) : a \in A\}$.

Inclusion Symbol
The symbol $\subset$ is called the inclusion symbol.

Index of a Subgroup
The number of left (or right) cosets of a subgroup H of a group G is called the

index of H in G and is denoted by $[G:H]$.

Indexed Family of Sets

Given a set I, if for each $\alpha \in I$, there is a set A_α, then $\{A_\alpha : \alpha \in I\}$ is called an indexed family of sets and the set I is called the indexing set.

Injective Mapping

If different elements in X have different images in Y under $f: X \to Y$, then f is called one-to-one mapping of X into Y. Such a mapping is also called the injective mapping.

Intersection of two Sets

The intersection of two sets A and B, denoted by $A \cap B$, is a set whose elements are in both A and B.

Inverse Element

The inverse of an element $x \in X$ with respect to $*$ is an element $x' \in X$ such that $x * x' = e = x' * x$, where e is the identity element of X.

Inverse Mapping

If $f: X \to Y$ is a bijective mapping, then we can find a rule $f^{-1}: Y \to X$ which assigns to each element y in Y a single element x in X. This rule is said to be the inverse mapping.

Inverse of Relation

The inverse of a binary relation R is a binary relation $R^{-1} = \{(b, a) : (a, b) \in R\}$.

Involution

An element of order 2 in a group G is called an involution.

Isomorphic Groups

Two groups G and G' are said to be isomorphic if there is an isomorphism $\phi: G \to G'$. In this case we write $G \approx G'$.

Isomorphism

A bijective homomorphism is called an isomorphism.

Kernel of Homomorphism

The kernel of homomorphism $\phi: G \to G'$ is the set of those elements of G whose image is the identity element of G'.

Lagrange's Theorem

The index and the order of a subgroup of a finite group divide the order of the group.

Left Coset

Let H be a subgroup of a group G and $a \in G$, then the set $aH = \{ah : h \in H\}$ is

said to be the left coset of H in G determined by a.

Monomorphism A one-one homomorphism is called a monomorphism.

Normal Subgroup A subgroup H of a group G is said to be self conjugate or normal subgroup of G if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

Normalizer $N(a) = \{x \in G : xa = ax\}$ is normalizer or centralizer of a in G.

Normalizer of a Complex Let X be an arbitrary complex in a group G, then the set of those elements of G which permute with X is called normalizer of X in G.

Null Set A set which contains no elements is called a null set. It is denoted by ϕ.

Nullary Relation A relation R from A to B is said to be empty or nullary if $R = \phi$.

Odd Permutation A permutation f in S_n is said to be an odd permutation if it can be written as a product of an odd number of transpositions.

Order of an Element If G is a group and $a \in G$, the order or period of a is the least positive integer n such that $a^n = e$.

Order of Group The number of elements in a group G is called the order of group G.

Order of Permutation The order of permutation f on a non-empty set X is the least positive integer n such that $f^n = I$, where I is the identity permutation.

Order or Degree of Rotation The number of rotations required for all the points to actually return to their original positions is called the order or degree of the rotation.

***p*-Group** A group G is said to be a p-group if the order of every element of G can be written as p^α, for some fixed p.

Partition of a Set A collection $\{A_\alpha : A_\alpha \subseteq A, \alpha \in I\}$ of subsets of A is said to be the partition of A if

(i) $A_\alpha \cap A_\beta = \phi$ if $\alpha \neq \beta$

(ii) $\bigcup_{\alpha \in I} A_\alpha = A$

Permutation
Let X be a non-empty set. A bijective mapping $f: X \to X$ is called the permutation on X.

Permutable Complexes
Two complexes X and Y in a group G are said to be permutable if $XY = YX$.

Proper Subset
If A is a subset of B and B has at least one element which is not in A, then A is called the proper subset of B.

Reflexive Relation
A relation R on a set A is said to be the reflexive relation if R contains the identity relation I.

Restriction of a Function
A function g is called an restriction of a function f if the domain of g is contained in the domain of f and $f(x) = g(x)$ for each x in the domain of g.

Right Coset
Let H be a subgroup of a group G and $a \in G$, then the set $Ha = \{ha : h \in H\}$ is said to be the right coset of H in G determined by a.

Semi Group
If G is a nonempty set then the order pair $(G, *)$ is said to be semi group if for all $a, b, c \in G$,

(i) $a * b \in G$, (ii) $a * (b * c) = (a * b) * c$.

Set
The collection of well defined objects is called a set.

Set Builder Method
If we describe a set by stating a characteristic property which identifies all the elements of the set then this method is said to be set builder method.

Sylow *p*-Subgroup
Let G be a group of order n and p a prime divisor of n. Subgroup H of G is said to be a *sylow p-subgroup* of G if H has order p^{α}, where p^{α} divides n and no other power of p divides n.

Sylow's First Theorem
A finite group whose order is divisible by a prime p, contains a sylow p-subgroup.

Sylow's Second Theorem
Any two sylow p-subgroups of a group are conjugate.

Sylow's Third Theorem
The number k of sylow p-subgroups of a finite group is congruent to 1 mod p and is a factor of the order of the group.

Subgroup
A subset H of a group G is called the subgroup of G if H itself is a group under

	the same binary operation as defined in G.
Subset	A set A is said to be the subset of a set B if every element of A is also an element of B.
Surjective Mapping	If the range, R_f, of a mapping $f: X \to Y$ is the set Y, then we call f a mapping of X onto Y. Such a mapping is also called the surjective mapping.
Symmetric Group	The group $(S_n, \circ)$ of permutations on X is called the symmetric group of degree n.
Symmetric Relation	A relation R on a set A is symmetric if and only if $R = R^{-1}$.
Transposition	A cycle of length two is called the transposition.
Trivial Subgroups	Every group G has at least two subgroups namely G itself and the identity group $\{e\}$. These are called the trivial subgroups of G. Any other subgroup of G is called a non-trivial subgroup of G.
Tabular Method	If we list the elements of the set by writing them within braces, then this method of writing a set is said to be the tabular method.
Transitive Relation	The relation R on A is said to be a transitive relation if $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ for all $a, b, c \in A$
Union of two Sets	The union of two sets A and B is a set whose elements are elements of A or of B.
Universal Set	If all the under consideration sets are assumed to be the subsets of a single fixed set then this fixed set is said to be the universal set and is usually denoted by U.
Vacuous Set	A set which contains no elements is called a vacuous set. It is denoted by ϕ.

*****

INDEX

Other Books of Mathematics

For

B.A / B.Sc. / BS 4-Years / M.Sc. Mathematics

By

Z. R. Bhatti

1. Laplace, Fourier and Z-Transforms
2. Introduction to Topology
3. Functional Analysis
4. Vector Analysis
5. Elementary Mathematics-I
6. Elementary Mathematics-II
7. Discrete Mathematics
8. Introduction to Integral Equations
9. An Introduction to Metric Spaces
10. Elementary Differential Equations
11. Introduction to Partial Differential Equations
12. Introduction to Linear Algebra
13. Objective General Mathematics
14. Solutions Manual of Laplace, Fourier and Z-Transforms
15. Solutions Manual of Introduction to Topology
16. Solutions Manual of Functional Analysis
17. Solutions Manual of Vector Analysis
18. Solutions Manual of Elementary Mathematics-I
19. Solutions Manual of Elementary Mathematics-II
20. Solutions Manual of Discrete Mathematics
21. Solutions Manual of Elementary Differential Equations
22. Solutions Manual of Introduction to Linear Algebra

*****